Courant Institute of
Mathematical Sciences

Elements of Algebraic Geometry

E. Artin

New York University

ELEMENTS OF ALGEBRAIC GEOMETRY

E. Artin

Spring 1955

Notes by G. Bachman
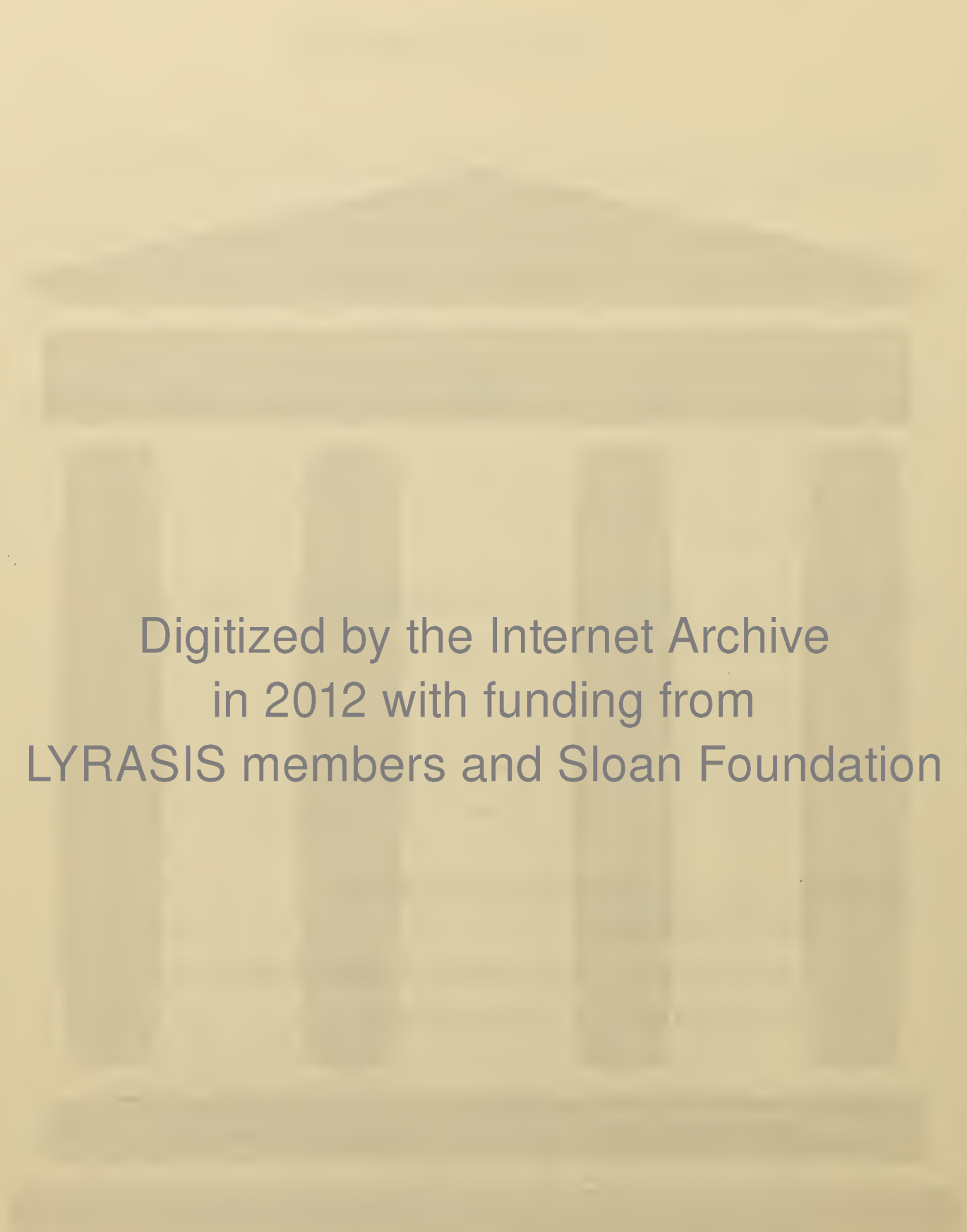
Courant Institute of Mathematical Sciences
New York University

Table of Contents

Introduction

These notes are based entirely on lectures given by Professor Artin during the spring semester-1955 at New York University. This part of the notes does not depend in any way on part I[*], but does assume a certain amount of familiarity with the basic concepts of modern algebra which can be found, for example, in Van der Waerden's Modern Algebra. Certain algebraic prerequisites will be presented in the introductory chapter of these notes while others will be presented in the later sections to which they are most relevant.

[*] Selected Topics in Geometry (out of print; will not be reprinted).
A revised edition will be published in the fall of 1956 by Interscience Publishers, Inc., New York, under the title "Geometric Algebra."

Chapter I

Basic Concepts of Algebraic Geometry

§1. **Noetherian Rings**: We begin our discussion with some algebraic prerequisites which will play an important role in our treatment of algebraic geometry. We will not isolate all the algebraic material required in this introductory chapter, but we will introduce most of it, as we progress, in the sections to which it most appropriately belongs. We now proceed towards the main aim of this section, namely, to prove the Hilbert Basis Theorem.

We assume throughout these notes, unless specific mention is made to the contrary, that all the rings which we will talk about are commutative and contain an identity element.

Definition 1.1: A ring $\mathscr{O}$ is called Noetherian if it satisfies the ascending chain condition for ideals.

That is, if a chain of ideals $\mathscr{O}_1, \mathscr{O}_2, \ldots$ is given in $\mathscr{O}$ such that

$$\mathscr{O}_1 \subseteqq \mathscr{O}_2 \subseteqq \mathscr{O}_3 \subseteqq \cdots ,$$

then there exists an integer i such that

$$\mathscr{O}_i = \mathscr{O}_{i+1} = \cdots .$$

2.

We observe that the ascending chain condition is equivalent to the maximal condition.

<u>Maximal condition</u>: Given any non-empty set S of ideals in $\mathcal{U}$, there exists an ideal $\mathcal{M} \in$ S which is maximal, i.e., $\mathcal{M}$ is contained in no other ideal of S.

The fact that the maximal condition implies the ascending chain condition is immediate. Conversely, if the ascending chain condition is satisfied but there exists a set S_1 of ideals not containing a maximal one, then we are immediately led to an ascending chain of ideals for which all the inclusions are proper which is a contradiction.

Finally, we wish to show that the ascending chain condition is equivalent to the basis condition.

<u>Basis Condition</u>: Every ideal in $\mathcal{U}$ has a finite basis, i.e., for any ideal $\mathcal{M} \in \mathcal{U}$, there exists a finite number of elements a_i, i = 1,...,ν, in the ideal $\mathcal{M}$ such that
$$\mathcal{M} = a_1 \mathcal{U} + \ldots + a_\nu \mathcal{U} .$$

We show first that the ascending chain condition implies the basis condition. Given any ideal $\mathcal{M} \in \mathcal{U}$, select $a_1 \in \mathcal{M}$, and form $a_1 \mathcal{U}$, i.e., the ideal generated by a_1. If $a_1 \mathcal{U} \neq \mathcal{M}$, take $a_2 \in \mathcal{M}$, but $a_2 \notin a_1 \mathcal{U}$, and form $a_1 \mathcal{U} + a_2 \mathcal{U}$. If this does not equal $\mathcal{M}$, select $a_3 \in \mathcal{M}$, but $a_3 \notin a_1 \mathcal{U} + a_2 \mathcal{U}$ etc. We are thus led to an ascending chain of ideals

3.

$$a_1\sigma \subseteq a_1\sigma + a_2\sigma \subseteq a_1\sigma + a_2\sigma + a_3\sigma \subseteq \cdots \quad .$$

Hence for some integer n we must have

$$a_1\sigma + a_2\sigma + \cdots + a_n\sigma = \sigma .$$

Now, conversely, suppose the basis condition is true in σ. Let

$$\mathcal{m}_1 \subseteq \mathcal{m}_2 \subseteq \cdots$$

be an ascending chain of ideals. Let $\mathcal{m} = \bigcup \mathcal{m}_i$. Then $\mathcal{m}$ is an ideal, for if $a, b \in \mathcal{m}$, then say $a \in \mathcal{m}_i$ and $b \in \mathcal{m}_j$. Hence $a, b \in \mathcal{m}_{\max(i,j)}$, so $a + b \in \mathcal{m}_{\max(i,j)} \subseteq \mathcal{m}$. While, if $a \in \mathcal{m}$, then say $a \in \mathcal{m}_i$. Then for any $c \in \sigma$, $ac \in \mathcal{m}_i$, so $ac \in \mathcal{m}$. Now, by assumption, $\mathcal{m}$ is finitely generated. Hence,

$$\mathcal{m} = a_1\sigma + \cdots + a_\nu\sigma .$$

Since $a_1 \in \mathcal{m}$, say $a_1 \in \mathcal{m}_{i_1}$. Similarly, $a_2 \in \mathcal{m}_{i_2}, \ldots,$ $a_\nu \in \mathcal{m}_{i_\nu}$. Hence, it follows that any $a_i, i = 1, \ldots, \nu$, belongs to $\mathcal{m}_j$ provided that j is larger than any i_ν. Consequently,

$$\mathcal{m} \subseteq \mathcal{m}_j \subseteq \mathcal{m}_{j+1} \subseteq \cdots \subseteq \mathcal{m} ,$$

so $\mathcal{m}_j = \mathcal{m}_{j+1} = \cdots$

which establishes the contention.

Now let us form $\sigma[X]$, the ring of polynomials in

X with coefficients in $\mathscr{O}$. Let $\mathscr{U}$ be an ideal of $\mathscr{O}[X]$. For each integer $n \geq 0$, we will construct an associated ideal $\mathscr{M}_n$ as follows:

$$\mathscr{U}_n = \left\{ a \;\middle|\; a \in \mathscr{O}, \; a \text{ coefficient of } X^n \text{ in some } f(X) \in \mathscr{U}; \; \deg f \leq n \right\}.$$

That is, we take all $f(X) \in \mathscr{U}$ of the form

$$f(X) = a_0 + a_1 X + \ldots + a_n X^n,$$

and the set of all a_n constitutes $\mathscr{M}_n$.

We observe that:

1) $\mathscr{M}_n$ is an ideal in $\mathscr{O}$.

2) $\mathscr{M}_n \subset \mathscr{M}_{n+1}$.

The first statement is clear, and the second follows from the fact that $\mathscr{O}$ contains an identity element and, hence, if $a_n \in \mathscr{M}_n$, then a_n appears as coefficient of X^{n+1} in $Xf(X) \in \mathscr{U}$, and, consequently, $a_n \in \mathscr{M}_{n+1}$.

Lemma 1.1: Let $\mathscr{U}$ and $\mathscr{B}$ be two ideals of $\mathscr{O}[X]$. If $\mathscr{U} \subset \mathscr{B}$, then $\mathscr{M}_n \subset \mathscr{b}_n$ for all n where $\mathscr{M}_n$ and $\mathscr{b}_n$ are the associated ideals of $\mathscr{U}$ and $\mathscr{B}$. Furthermore, if, in addition, $\mathscr{M}_n = \mathscr{b}_n$ for all n, then $\mathscr{U} = \mathscr{B}$.

Proof: The first part of the lemma is obvious; we proceed to establish the second part. Let

$$f(X) = b_0 + \ldots + b_n X^n \in \mathscr{B}.$$

We wish to show that $f(X) \in \mathcal{U}$. The proof will go by induction. If n = 0, then

$$f(X) \in \mathcal{b}_o = \mathcal{A}_o \subset \mathcal{U}.$$

We assume the statement true for polynomials of degree n - 1, and show its validity for those of degree n. Since $f(X) \in \mathcal{B}$, we have

$$b_n \in \mathcal{b}_n = \mathcal{A}_n.$$

Therefore, there exists a polynomial $g(X) \in \mathcal{U}$ such that

$$g(X) = a_o + a_1 X + \ldots + b_n X^n.$$

But, since $\mathcal{U} \subset \mathcal{B}$, we have $g(X) \in \mathcal{B}$. Thus $f(X) - g(X) \in \mathcal{B}$, and $\deg(f(X) - g(X)) \leq n-1$, so, by induction, $f(X) - g(X) \in \mathcal{U}$, and, since $g(X) \in \mathcal{U}$, we have $f(X) \in \mathcal{U}$ which finishes the lemma.

We are now in a position to state and prove the important theorem due to Hilbert.

Theorem 1.1 (Hilbert Basis Theorem): If $\mathscr{r}$ is a Noetherian ring, then $\mathscr{r}[X]$ is also a Noetherian ring.

Proof: We consider the ascending chain of ideals

$$\mathcal{U}_1 \subset \mathcal{U}_2 \subset \mathcal{U}_3 \subset \ldots$$

in $\mathscr{r}[X]$. We form the associated ideals $\mathcal{U}_{ij}$ to the ideals $\mathcal{U}_i$, and we obtain the following "pattern" of inclusions:

$$
\begin{array}{ccccccc}
\vdots & & \vdots & & \vdots & & \\
\cup & & \cup & & \cup & & \\
\mathcal{M}_{30} & \subset & \mathcal{M}_{31} & \subset & \mathcal{M}_{32} & \subset & \cdots \\
\cup & & \cup & & \cup & & \\
\mathcal{M}_{20} & \subset & \mathcal{M}_{21} & \subset & \mathcal{M}_{22} & \subset & \cdots \\
\cup & & \cup & & \cup & & \\
\mathcal{M}_{10} & \subset & \mathcal{M}_{11} & \subset & \mathcal{M}_{12} & \subset & \cdots
\end{array}
$$

Considering the diagonal chain $\mathcal{M}_{10}, \mathcal{M}_{21}, \mathcal{M}_{32}, \ldots$,
we get an ascending chain the ideals of which must all
become equal after a finite number of proper inclusions.
Thus, diagrammatically, we have the following situation:
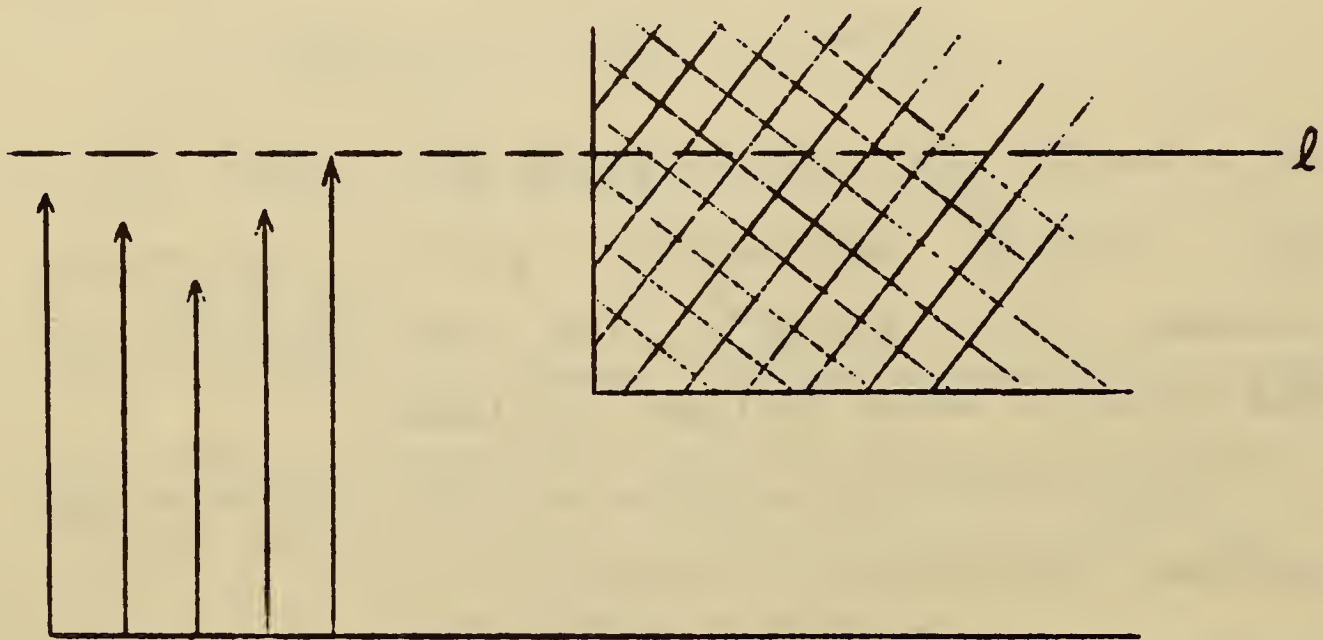
All the ideals situated in the shaded region are equal;
there are only a finite number of vertically increasing
chains of ideals to the left of this region tne ideals
of which must become equal after a finite number of
inclusions. This is indicated in the diagram by the

arrow heads at various heights. Thus we are sure that for every vertically increasing chain, after a finite number of inclusions, all ideals in the chain become equal. The line ℓ indicates that above it the vertical inclusions become equalities. Now applying lemma 1.1, we get that the corresponding ideals in $\mathscr{O}[X]$ are equal, and, hence $\mathscr{O}[X]$ is Noetherian.

As an immediate corollary, we have

Corollary 1.1: If $\mathscr{O}$ is a Noetherian ring, then $\mathscr{O}[X_1,\ldots,X_n]$ is a Noetherian ring.

If $\mathscr{O} = k$ is a field, then k contains only the trivial ideal, (0), and the ideal k = (1). Thus we get:

Corollary 1.2: If k is a field, then $k[X_1,\ldots,X_n]$ is a Noetherian ring.

§2. Introductory concepts of algebraic geometry: We proceed, at first, in this section in an heuristic manner. We want to consider the common solutions of the following polynomial equations:

(2.1)

$$f_1(X_1,\ldots,X_n) = 0$$
$$f_2(X_1,\ldots,X_n) = 0$$
$$\cdots \cdots \cdots$$
$$\cdots \cdots \cdots$$
$$f_r(X_1,\ldots,X_n) = 0 \, .$$

If the coefficients of these polynomials belong to the complex number field, we will refer to this as the classical case. In general, we permit the coefficients to belong to an arbitrary commutative field: denoted by k.

The next question which presents itself is: where are we to take the solutions from? In order to obtain any degree of generality, it is evident that we shouldn't restrict the solutions to lie in k; for example, if k = R, the field of rational numbers, then $X_1^2 + X_2^2 + 1 = 0$ has no solution in R. It is, therefore, apparent that to obtain any amount of generality we must permit ourselves to take solutions the components of which lie in an extension field of k and which is algebraically closed. We could stop here, however, this is still not general enough for our purposes, for throughout these notes we will want to consider "sufficiently general" points belonging to the set of common zeros of a set of polynomial equations. Thus it will be necessary to take an extension field Ω of k which is not only algebraically closed, but is such that the degree of transcendency of Ω over k is infinite. The two points of view, namely, whether we take the components of the solutions from the algebraic closure of k, or from Ω, as defined above, will be resolved when we consider, later in these notes, the Hilbert Nullstellensatz. Summarizing, we will take

the components of the solutions from the <u>universal domain</u> Ω where Ω is an extension field of k such that:

1) The degree of transcendency of Ω/k is infinite, and

2) Ω is algebraically closed.

If a solution of (2.1) lies in k itself, we will call it a <u>rational solution</u>, and if a solution of (2.1) is algebraic over k, we will call it an <u>algebraic solution</u>.

We shall now see that any "reasonable" extension field of k can be "accommodated" in Ω. To be precise, we prove:

<u>Theorem 2.1</u>: Let $k \subset E$, and let $E = k(a_1, \ldots, a_r)$, Then there exists an isomorphism $\sigma : E \longrightarrow \Omega$ which is identity on k.

<u>Proof</u>: Put $k_{r-1} = k(a_1, \ldots, a_{r-1})$, and let $k_o = k$. Then $E = k_r = k_{r-1}(a_r)$. The proof proceeds by induction. For $r = 0$, the statement to be proved is trivial. Suppose the theorem is true for $s < r$. Then there exists an isomorphism

$$\sigma_{r-1} : k_{r-1} \longrightarrow k'_{r-1} \subset \Omega$$

which is identity on k. There are two cases:

1) a_r is transcendental over k_{r-1}. Then select in Ω an element β_r which is transcendental over k'_{r-1}. This

can be done since Ω has infinite degree of transcendency over k while k_{r-1}' has only a finite degree of transcendency over k. Now extend σ_{r-1} to E by mapping a_r onto β_r. As is well-known, this extension is an isomorphism which leaves k fixed.

2) a_r is algebraic over k_{r-1}. Let

$$P = I_{rr}(a_r, k_{r-1}),$$

that is, P is the irreducible equation over k_{r-1} satisfied by a_r. Let P' be its image in k_{r-1}'. Select $\beta_r \in \Omega$ as root of P'. This can be done since Ω is algebraically closed. Now we extend the isomorphism σ_{r-1} to an isomorphism of E into Ω which leaves k fixed by mapping a_r onto β_r. That this is an isomorphism is a well-known result of modern algebra. Hence, the theorem is true for s = r which concludes the proof.

Now let us return to the original discussion which started this section. We took polynomials $f_1, f_2, \ldots f_r \in k[X]$ where $X = (X_1, \ldots, X_n)$, and agreed to take common solutions $(x) = (x_1, \ldots, x_n)$ from Ω^n where $\Omega^n = \Omega \times \ldots \times \Omega$. But, we observe, that if (x) is a zero for $f_1, f_2, \ldots, f_r$, then (x) is also a zero for $g_1 f_1 + \ldots + g_r f_r$ where the g_i are arbitrary polynomials of k[X]. Thus (x) is a zero of the ideal generated by $f_1, f_2, \ldots, f_r$. Thus instead of considering the original problem we consider the following:

given an ideal $\mathcal{A} \subset k[X]$ where $X = (X_1, \ldots, X_n)$ investigate the zeros (x) of $\mathcal{A}$ where $(x) = (x_1, \ldots, x_n) \in \Omega^n$, and where (x) is called a zero of $\mathcal{A}$ if for every $f(X) \in \mathcal{A}$, we have $f(x) = 0$. This problem is actually equivalent to our original problem since, by the Corollary 1.2, any ideal $\mathcal{A}$ of $k[X]$ is finitely generated, so to find a zero of $\mathcal{A}$ it suffices to find a zero of only a finite number of elements of $\mathcal{A}$.

Definition 2.1: Let $\mathcal{A}$ be an ideal of $k[X]$. The set of zeros of $\mathcal{A}$ is called an algebraic set (we also say that $\mathcal{A}$ defines an algebraic set) over k.

We observe that some authors refer to an algebraic set as a variety, and then call what we will call a variety an irreducible variety.

To designate that an ideal $\mathcal{A}$ defines an algebraic set, say S, we will write: $\mathcal{A} \longrightarrow S$. We note that S can be the empty set ϕ; this is true when $\mathcal{A} = k[X]$, since then the identity element $1 \in \mathcal{A}$. Also, $S = \Omega^n$ when $\mathcal{A} = (0)$, the zero ideal. It is also possible for different ideals to define the same algebraic set.

We observe trivially:

Lemma 2.1: If $\mathcal{A}$ and b are ideals, then $\mathcal{A} \subset b \implies V \supset W$ where $\mathcal{A} \longrightarrow V$, and $b \longrightarrow W$.

We now wish to show that the class of algebraic sets is closed under union and intersection. To be exact, we show:

Theorem 2.2: If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals, and if $\mathfrak{a} \rightarrow V$, and $\mathfrak{b} \rightarrow W$, then $V \cup W$ and $V \cap W$ are algebraic sets. Moreover, $\mathfrak{a} + \mathfrak{b} \rightarrow V \cap W$, and both the ideals $\mathfrak{a}\mathfrak{b}$ and $\mathfrak{a} \cap \mathfrak{b}$ define $V \cup W$.

Proof: The fact that $\mathfrak{a} + \mathfrak{b} \rightarrow V \cap W$ is immediate. We proceed to the second statement. Let $\mathfrak{a} \cap \mathfrak{b} \rightarrow S$, and $\mathfrak{a}\mathfrak{b} \rightarrow R$. Since $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{a}$, and $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{b}$, we have, by lemma 2.1, that $S \supset V$, and $S \supset W$. Consequently,

$$(2.1) \qquad\qquad S \supset V \cup W.$$

Now we show that any zero of $\mathfrak{a}\mathfrak{b}$ is in $V \cup W$. Let (x) be a zero of $\mathfrak{a}\mathfrak{b}$, and suppose $(x) \notin V$; we wish to show that $(x) \in W$. By assumption, (x) is not a zero of $\mathfrak{a}$. Hence, there exists an $f(X) \in \mathfrak{a}$ such that $f(x) \neq 0$. Let $g(X)$ be any element of $\mathfrak{b}$; then $f(X)g(X) \in \mathfrak{a}\mathfrak{b}$. Therefore, $f(x)g(x) = 0$ which implies that $g(x) = 0$, i.e., $(x) \in W$. Finally we observe that $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$; whence, $R \supset S$. Combining (2.1) with the statement following it, we have

$$V \cup W \supset R \supset S \supset V \cup W.$$

Thus $R = S = V \cup W$, and theorem 2.2 has been established in full.

§3. Varieties and generic points:

Definition 3.1: An algebraic set V is called a variety if V is not a proper union of a finite number of algebraic sets.

Using theorem 2.2, we can say, therefore, that an algebraic set V is a variety if V is not a proper union of two algebraic sets. That is, if V is a variety, and $V = W \cup U$ where W and U are algebraic sets, then either $U = V$ or $W = V$.

Now let S be <u>any</u> set in Ω^n. To S, we associate an ideal $\mathcal{M}$ of k[X] as follows:

$$\mathcal{M} = \left\{ f(X) \,|\, f(X) \in k[X]; \ f(S) = 0 \right\} .$$

That is, $\mathcal{M}$ consists of those elements of k[X] which vanish for all points of S. We observe:

1) $\mathcal{M}$ is an ideal. The proof is trivial.

2) If S is an algebraic set defined by $\mathcal{M}_0$, then the associated ideal $\mathcal{M}$ of S is the largest defining ideal of S.

To prove this, we observe that $\mathcal{M}_0 \subset \mathcal{M}$, for, since $\mathcal{M}_0 \rightarrow S$, we have if $f \in \mathcal{M}_0$, then $f(S) = 0$; thus $f \in \mathcal{M}$, so $\mathcal{M}_0 \subset \mathcal{M}$. Now let $\mathcal{M} \rightarrow R$. Since $\mathcal{M}_0 \subset \mathcal{M}$, we have $S \supset R$. But $R \supset S$, by the definition of $\mathcal{M}$. Consequently, $R = S$; whence $\mathcal{M}$ is the largest defining ideal of S.

If S is an algebraic set, and $\mathcal{M}$ the associated ideal, or, as we will also say, the determined ideal, (hence the largest defining ideal of S), we denote this association by: $S \rightarrow \mathcal{M}$.

If we restrict ourselves to the largest defining ideals, then the converse of lemma 2.1 holds, namely:

Lemma 3.1: Let V, W be algebraic sets, and let $\mathcal{m}, b$ be the largest defining ideals of V, W respectively. Then $V \supset W \Rightarrow \mathcal{m} \subset b$.

Proof: $f \in \mathcal{m} \Rightarrow f(V) = 0 \Rightarrow f(W) = 0 \Rightarrow f \in b$.

Combining lemmas 2.1 and 3.1 and the preceding discussion, we know that there is a one-to-one lattice inverting correspondence between algebraic sets and certain ideals, namely, the largest defining ideals. Also, we observe that since k[X] is Noetherian, it follows that every desceding chain of algebraic sets breaks off, or, in other words, the minimal condition is satisfied for algebraic sets.

We will now prove the important theorem:

Theorem 3.1: Any non-empty algebraic set is the union of a finite number of varieties.

Proof: We consider the set $\sum$ of all algebraic sets which do not satisfy the statement of the theorem; that is, $\sum$ consists of those algebraic sets which are not a finite union of varieties. We wish to show that $\sum = \phi$, the empty set. Assume that $\sum$ is not empty, and let V be a minimal set of $\sum$, and $V \neq \phi$. Then, by definition, V is not a variety. Hence,

(3.1) $$V = U \cup W$$

where U, W are algebraic sets, a d $U \neq V$, and $W \neq V$. It follows, by the choice of V, that $U \notin \sum$, and $W \notin \sum$.

Thus U is a finite union of varieties, and W is a finite union of varieties. Consequently, V is a finite union of varieties by (3.1); whence, $V \in \sum$ which is a contradiction, so $\sum$ is empty.

Theorem 3.1 shows that every algebraic set V can be written as:

$$(3.2) \qquad V = W_1 \cup W_2 \cup \ldots \cup W_r$$

where the W_i, $i = 1, \ldots, r$, are varieties. It is not true, however, that this representation is unique since, for example, it is possible that $W_2 \subset W_1$ in which case W_2 can be omitted from the representation (3.2) yielding another representation. If, however, we assume that it is never true that $W_i \subset W_j$ for $i \neq j$, then we can show that the representation (3.2) is unique. In order to prove this, we first prove the following:

Lemma 3.2: Let U be a variety and let V be an algebraic set with the representation (3.2). If $U \subset V$, then there exists an integer i such that $U \subset W_i$.

Proof:

$$\begin{aligned}
U &= U \cap V \\
(3.3) \\
&= U \cap W_1 \cup [(U \cap W_2) \cup \ldots \cup (U \cap W_r)].
\end{aligned}$$

But by theorem 2.2 we know that the class of algebraic sets is closed under union and intersection. Thus (3.3) yields:

variety U = union of two algebraic sets

from which it follows, by repetition, that there exists

an integer i such that $U = U \cap W_i$, or $U \subseteq W_i$.

Now let us show the uniqueness of the representation

(3.2) under the added assumption that $W_i \not\subset W_j$ for $i \neq j$.

Suppose we also have:

$$V = U_1 \cup U_2 \cup \ldots \cup U_s$$

where U_i, $i = 1, \ldots, s$, is a variety and $U_i \not\subset U_j$ for $i \neq j$.

Since $U_i \subset V$, we have by lemma 3.2 that there exists an

integer j such that $U_i \subset W_j$, and, similarly, there exists

an integer r such that $W_j \subset U_r$, so

$$U_i \subset W_j \subset U_r$$

whence, by assumption, $i = r$, and, therefore, $U_i = W_j$.

Thus each U_i occurs among the W_j, and, similarly, each W_j

occurs among the U_i, so we have uniqueness.

We have seen already that there is a one-to-one

lattice inverting correspondence between algebraic sets

and their largest defining ideals. We now wish to show

that the varieties are in one-to-one correspondence with

the prime ideals of $k[X]$. We first show:

<u>Theorem 3.2</u>: If V is a variety, then $V \rightarrow \mathscr{Y}$ where $\mathscr{Y}$ is

a prime ideal (i.e., those polynomials of $k[X]$ which

vanish on all of V form a prime ideal).

Proof: Suppose $\mathfrak{p}$ is not a prime ideal. Then there exist $a, b \in \mathcal{O} = k[X]$ such that $ab \in \mathfrak{p}$, and $a \notin \mathfrak{p}$, and $b \notin \mathfrak{p}$. Set

$$\mathfrak{a} = \mathfrak{p} + a\mathcal{O}.$$

Then $\mathfrak{a} \supset \mathfrak{p}$ properly since $a \notin \mathfrak{p}$, and

$$\mathfrak{a} \longrightarrow U \subset V$$

where the inclusion is proper since $\mathfrak{p}$ is the largest ideal defining V. Similarly, we set

$$\mathfrak{b} = \mathfrak{p} + b\mathcal{O}.$$

Then $\mathfrak{b} \supset \mathfrak{p}$ properly, and $\mathfrak{b} \longrightarrow W \subset V$ where the inclusion is proper. Thus $U \cup W \subset V$. Now

$$\mathfrak{a}\,\mathfrak{b} = (\mathfrak{p} + a\mathcal{O})(\mathfrak{p} + b\mathcal{O})$$
$$= \mathfrak{p}^2 + a\mathfrak{p} + b\mathfrak{p} + ab\mathcal{O},$$

so

$$\mathfrak{a}\,\mathfrak{b} \subset \mathfrak{p},$$

but $\mathfrak{a}\,\mathfrak{b} \longrightarrow U \cup W$, and thus $U \cup W \supset V$. Hence, $V = U \cup W$ where $U \subset V$, and $W \subset V$ properly which contradicts the fact that V is a variety, and, therefore, theorem 3.2 has been established.

We now wish to show that any prime ideal $\mathfrak{p}$ determines a variety which, in turn, determines the given ideal $\mathfrak{p}$. Suppose, then, that $\mathfrak{p}$ is a given prime ideal defining an algebraic set V. If $\mathfrak{p} = \mathcal{O} = k[X]$, then the algebraic set

is ϕ which is a variety, and there is nothing to prove.
Hence, we may assume that $\mathscr{a} \neq \mathscr{o}$. Let κ denote the
canonical map of $\mathscr{o} = k[X]$ (where, as usual, $X = (X_1, \ldots, X_n)$)
onto $\mathscr{o}/\mathscr{a}$:

$$\mathscr{o} = k[X] \xrightarrow{\kappa} \mathscr{o}/\mathscr{a} .$$

Since $\mathscr{o}/\mathscr{a}$ is a domain of integrity, we can form its
quotient field $\overline{K}$. Let i denote the isomorphism of $\mathscr{o}/\mathscr{a}$
into F :

$$\mathscr{o}/\mathscr{a} \xrightarrow{i} \overline{K}.$$

Now consider $\kappa | k$, i.e., the restriction of the canonical
map to k. This gives a homomorphism of k, and is, there-
fore, either trivial or an isomorphism, but since $\mathscr{o} \neq \mathscr{a}$,
we have $1 \notin \mathscr{a}$, and, consequently, 1 does not go into 0
under κ. Hence $\kappa | k$ is not trivial but is an isomorph-
ism into. Let $\overline{k}$ denote the image of k under $\kappa | k$, so
$\overline{k} \simeq k$. Finally, let X go into $(\overline{x})$ (where $(\overline{x}) = (\overline{x}_1, \ldots, \overline{x}_n)$)
by the canonical map. Then $\mathscr{o}/\mathscr{a} = \overline{k}[\overline{x}]$, so $\overline{K} = \overline{k}(\overline{x})$.
Now, by the properties of Ω, we can find an $(x) \in \Omega^n$
such that the obvious map $r : \overline{k}(\overline{x}) \longrightarrow k(x)$ is an iso-
morphism (on $\overline{k}$, r is the given isomorphism, and r takes
$\overline{x}$ into x). r is called the realization in Ω. Thus we
have the following sequence of maps:

$$k[X] \xrightarrow{\kappa} \overline{k}[\overline{x}] \xrightarrow{i} \overline{k}(\overline{x}) \xrightarrow{r} k(x).$$

Hence we have a homomorphism: $k[X] \longrightarrow k(x)$ whose kernel is $\mathfrak{p}$, so $(x) \in V$. As we shall see presently, we have obtained the existence of a generic point for a non-empty variety.

Now consider the set consisting of the one point (x). As we have just seen: $(x) \longrightarrow \mathfrak{p}$. Let $V \longrightarrow \mathfrak{m}$. Since $(x) \subset V$, we have $\mathfrak{p} \supset \mathfrak{m}$, but $\mathfrak{m}$ is the largest ideal which can define V; hence $\mathfrak{m} \supset \mathfrak{p}$, so $\mathfrak{m} = \mathfrak{p}$. Recapitulating, we have shown that starting with a prime ideal $\mathfrak{p}$ which defines an algebraic set V, then this V determines $\mathfrak{p}$ (i.e. V determines a largest defining ideal which is $\mathfrak{p}$). Now we will show that the algebraic set V is actually a variety. Suppose

$$V = U \cup W$$

where U, W are algebraic sets such that $\mathfrak{a} \longrightarrow U$, and $\mathfrak{b} \longrightarrow W$. Then $\mathfrak{a}\mathfrak{b} \longrightarrow U \cup W = V$, so $\mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$ since $\mathfrak{p}$ is the largest ideal defining V. Now if $\mathfrak{a} \not\subset \mathfrak{p}$, then there exists an $a \in \mathfrak{a}$ such that $a \not\subset \mathfrak{p}$, but $ab \in \mathfrak{p}$ for any $b \in \mathfrak{b}$; consequently, $\mathfrak{b} \subset \mathfrak{p}$, so either $\mathfrak{a} \subset \mathfrak{p}$, or $\mathfrak{b} \subset \mathfrak{p}$. Hence, either $U \supset V$, or $W \supset V$. Therefore, either $U = V$ or $W = V$, so V is a variety.

Combining theorem 3.2 with the preceding discussion gives:

Theorem 3.3: The varieties of Ω^n are in one-to-one correspondence with the prime ideals of $k[X]$.

We also mentioned in the discussion that we obtained the existence of a generic point for a non-empty variety. By this, we mean:

<u>Definition 3.1</u>: Let V be a non-empty variety determined by the prime ideal $\wp$. Let $(x) \in V$. (x) is called a generic point of V if the ideal determined by the set consisting of just (x) is $\wp$ (i.e., $(x) \longrightarrow \wp \longrightarrow V$).

We observe, first of all, that if (x) is a generic point of the variety V, then V is the smallest algebraic set containing (x). For suppose $(x) \in W$ where W is an algebraic set, and $\mathfrak{A} \longrightarrow W$. Then $\mathfrak{A}(x) = 0$ (i.e., (x) is a zero of the ideal $\mathfrak{A}$), but this implies that $\mathfrak{A} \subset \wp$, so $W \supset V$.

Next, we note that any point is a generic point of some variety. Let (x) be any point in Ω^n. Let $\wp$ be the ideal defined by the set consisting of this one point. Then $\wp \neq \mathfrak{O}$ since 1 doesn't vanish for (x). Furthermore, $\wp$ is a prime ideal, for suppose $f(X)g(X) \in \wp$. Then $f(x)g(x) = 0$. Suppose $f(X) \notin \wp$, i.e., $f(x) \neq 0$. Then $g(x) = 0$, so $g(X) \in \wp$. Thus $\wp$ is a prime ideal not equal $\mathfrak{O}$, but we know that then $\wp$ defines a variety, and (x) is a point of this variety. Moreover, (x) satisfies the conditions of Definition 3.1, so it is a generic point of the variety V.

Before proceeding further with the general discussion, we will consider a few examples in order to illustrate the

concepts that we have introduced.

We take $k = Q$, the field of rational numbers, and $\Omega = C$, the complex numbers. We wish to determine the varieties in Ω^2 of which the following points are generic points: $(e, e^{\sqrt{2}})$, (e,e), $(\sqrt{2}, 1)$, $(0,0)$.

1) $(e, e^{\sqrt{2}})$. Since e and $e^{\sqrt{2}}$ are independent transcendental elements the ideal $\mathcal{Y}$ of $\mho = Q[X_1, X_2]$ determined by $(e, e^{\sqrt{2}})$ is (0), the null ideal, which defines the variety Ω^2. Thus $(e, e^{\sqrt{2}})$ is a generic point of Ω^2, and Ω^2 is the smallest algebraic set containing $(e, e^{\sqrt{2}})$.

2) (e,e). Here, we must consider those $f(X_1, X_2) \in \mho$ such that $f(e,e) = 0$. It is easy to see that the prime ideal $\mathcal{Y}$ determined by (e,e) is $\mathcal{Y} = (X_1 - X_2)$ (the principal ideal generated by $X_1 - X_2$), and thus the variety of which (e,e) is a generic point is $\{(x_1, x_2) | x_1 = x_2\}$.

3) $(\sqrt{2}, 1)$. Here, it is easy to see that

$$\mathcal{Y} = (X_1^2 - 2)\mho + (X_2 - 1)\mho ,$$

so that the variety of which $(\sqrt{2}, 1)$ is a generic point is $\{(\sqrt{2}, 1), (-\sqrt{2}, 1)\}$. We note that both $(\sqrt{2}, 1)$ and $(-\sqrt{2}, 1)$ are generic points of this variety.

4) $(0,0)$. Here, $\mathcal{Y}$ consists of those polynomials of $\mho$ with no constant term, and the variety of which $(0,0)$ is generic point is just the point $(0,0)$. In fact, if we took instead of $(0,0)$ any point (r_1, r_2) where

$r_1, r_2 \in Q$, we would get that the variety of which it is a generic point is just the point (r_1, r_2).

Now let us go back to the general discussion. The next concept which we wish to define is that of the dimension of a variety.

Definition 3.2: Let V be a variety, and let (x) be a generic point. Then the dimension of V is: dim V = $[k(x):k]_{tr}$ (i.e., the degree of transcendency of k(x) over k).

Instead of dim V, we will also write dim(x). We observe that for the illustrative examples: in case 1), the dimension of the variety is 2; in case 2), the dimension of the variety is 1; while in cases 3) and 4), the dimension is 0.

We must show that the definition of dimension is independent of the particular generic point chosen. We will do this presently, but first we must show how the other points of a variety are related to a generic point.

Let V be a variety and (x) a generic point of V. Consider the obvious map:

$$\eta : k[X] \longrightarrow k(x)$$

(η is identity on k and takes X into x). Clearly, η is a homomorphism with kernel $\wp$. Let $(z) \in \Omega^n$, and consider the obvious map

$$\nu : k[x] \longrightarrow k[z].$$

Clearly, v is a homomorphism if it is well-defined, so
we must see if v is well-defined. That is, we must have
$f(x) = g(x) \implies f(z) = g(z)$, or it suffices to have
$f(x) = 0 \implies f(z) = 0$. But $f(x) = 0$ means $f(\lambda) \in \mathscr{Y}$, so
the map v is well-defined if and only if $\mathscr{Y}(z) = 0$. Thus
the map v is well-defined and consequently a homomorphism
for all $(y) \in V$. Hence, we can say the points of the
variety V for which (x) is the generic point are exactly
those for which the obvious map $v:k[x] \longrightarrow k[y]$ is well-
defined and, therefore, a homomorphism. We call this
procedure a specialization, i.e.,

Definition 3.3: (y) is called a specialization of the
generic point (x) if the obvious map $v:k[x] \longrightarrow k[y]$ is
well-defined.

If (y) is a specialization of (x), we will denote
this by: $(x) \longrightarrow (y)$. We also observe that in terms of
specializations we can say that the points of the variety
V, whose generic point is (x), consist of the speciali-
zations of (x).

Let $(x) \longrightarrow (y)$. Since, as we've seen, any point
(y) is a generic point of some variety, we may consider
specializations of (y). e claim:

Lemma 3.3: $(x) \longrightarrow (y) \longrightarrow (z) \implies (x) \longrightarrow (z)$.

Proof: If a polynomial relation holds in (x), then,
by assumption, it holds in (y), and, therefore, by

assumption in (z), so, indeed, (x) ⟶ (z).

Let us now see what (y) ⟶ (x) and (x) ⟶ (y) means. In this case, we have:

$$k[X] \xrightarrow{\eta} k[x] \longleftrightarrow k[y].$$

Here, the map ν is an isomorphism since it is well-defined in both directions, so the kernels of the homomorphisms k[X] ⟶ k[x], and k[X] ⟶ k[y] are the same, so that (x) and (y) are generic points of the same variety. We call them _equivalent_ generic points.

Finally, we show that dim V is independent of the choice of the generic point. This is clear since for any two generic points (x) and (y) of V, we have the iso-morphic rings: $k[x] \simeq k[y]$; thus $k(x) \simeq k(y)$ by the obvious map, so the degree of transcendency computed with the generic point (x) is the same as that computed with the generic point (y).

The next concept which we want to introduce is that of a _subvariety_. We say that W is a subvariety of the variety V if W is a variety and if W is a subset of V. The first observation which we wish to make concerning subvarieties is the following: any point of the variety V can be considered as a generic point of a subvariety. That is, let (x) define V, and let (y)∈V, then (y) defines a subvariety W, for (x) ⟶ (y), but the speciali-zations (y) ⟶ (z) form the points of W, and, by lemma

3.3, these are points of V.

Now, we wish to relate the dimension of a variety with that of a subvariety. We prove the important theorem:

<u>Theorem 3.4</u>: Let W, V be varieties. Suppose $W \subset V$; then $\dim W \leq \dim V$, and $\dim W = \dim V$ implies that $W = V$.

<u>Proof</u>: Let $(x) = (x_1, \ldots, x_n)$ be a generic point of V, and let $(y) = (y_1, \ldots, y_n)$ be a generic point of W. Then the obvious map $\phi : k[x] \longrightarrow k[y]$ is well-defined. Suppose $\dim W = r$. There is no loss of generality in assuming that $y_1, y_2, \ldots, y_r$ are algebraically independent elements over k. Then $x_1, x_2, \ldots, x_r$ are algebraically independent, for otherwise some polynomial $f(x_1, \ldots, x_r) = 0$ with coefficients which are in k and not all zero. Therefore, since ϕ is well-defined, we have $f(y_1, \ldots, y_r) = 0$ which is a contradiction, so $\dim V \geq r$. Now assume that $\dim V = r$. We wish to show that then $(y) \longrightarrow (x)$, or, i.e., ϕ is an isomorphism. Let $z \in k[x]$ and $z \neq 0$; assume that z is in the kernel of ϕ. z is algebraically dependent on $x_1, \ldots, x_r$ since, by assumption, $\dim V = r$. Consequently, we must have

(3.4) $\qquad a_s(x_1, \ldots, x_r) z^s + \ldots + a_0(x_1, \ldots, x_r) = 0$

where the $a_i(x_1, \ldots, x_r)$ are polynomials with coefficients in k and not all are zero. If we assume that s is the minimal degree for all such equations satisfied by z, then $a_0(x_1, \ldots, x_r) \neq 0$. Applying ϕ to (3.4) we obtain

$a_0(y_1,\ldots,y_r) = 0$ which contradicts the fact that $y_1,\ldots,y_r$ are algebraically independent. Hence the kernel is zero, so both (x) and (y) are generic points of V, so $' = V$.

Now we wish to consider some special values of dim V. First, we note that dim $V = \max\limits_{(x)\in V} \dim(x)$ where, for any $(x)\in V$, $\dim(x) = [k(x):k]_{tr}$. Secondly, we observe that

$$0 \le \dim V \le n.$$

Let us consider the case dim $V = n$.

case 1) $\underline{\dim V = n}$. Let (x) be a generic point of V. Then $x_1, x_2, \ldots, x_n$ must be algebraically independent. Thus any $(y)\in \Omega^n$ is a specialization of (x) since no polynomial relation can hold in $k[x]$, so in this case $V = \Omega^n$. Consequently, Ω^n has dimension n, and any proper subset has dimension less than n.

case 2) $\underline{\dim V = 0}$. Then (x) is algebraic, i.e., each x_1 is algebraic over k. Let (y) be a specialization of (x): $(x) \longrightarrow (y)$. Then, as we've seen, (y) is a generic point of a subvariety W: $V \supset W$. Thus $0 = \dim V \ge \dim V$, so dim $= 0$ which implies, by theorem 3.4, that $V = W$. Therefore, (y) is also a generic point of V. Hence, in this case, every specialization is an equivalent generic point. Thus if $(x) \longrightarrow (y)$, then $k[x] \simeq k[y]$. But here $k[x] = k(x)$. This follows from the following facts:

a) $k[x]$ is a finite dimensional vector space. This is clear for $k[x]$ is spanned by the totality of $x_1^{v_1} \ldots x_n^{v_n}$, and since each x_i is algebraic we can replace higher powers by lower ones.

b) $k[x]$ is a domain of integrity. This is likewise clear since k is a domain of integrity.

c)[*] A finite dimensional vector space over a field which is a domain of integrity is a field. For let R be a finite dimensional vector space over a field, and let R be a domain of integrity. Let $a \in R$, and $a \neq 0$. Consider the map: $x \longrightarrow ax$ for all $x \in R$. Clearly, this map is an isomorphism of R into R, and, since it preserves dimension, it is an onto map. Therefore, the equation $ax = \beta$, $a, \beta \in R$ always has an unique solution $x \in R$.

Combining a), b), c), we have $k[x] = k(x)$, so, in this case, the specializations of (x) are just those $(y) \in \Omega^n$ such that $k(x) \simeq k(y)$. That is, when dim $V = 0$, V has as many points as there are isomorphisms of $k(x)$ over k. Thus, if dim $V = 0$, the number of points of V is at most the degree of $k(x)$ over k. If all x_i are separable, then the number of points equals the degree of $k(x)$ over k.

case 3) dim V = n-1. As we know, the varieties are in one-to-one correspondence with the prime ideals, so

---

[*] In a similar manner, one shows: If $\mathcal{U}$ is a ring without divisors of zero satisfying the minimal condition for right and left ideals, then $\mathcal{U}$ is a field - see van der Waerden, Modern Algebra, Vol.II, p. 139.

$V \longleftrightarrow \mathcal{Y}$ where $\mathcal{Y} \neq (0)$ since $V \neq \Omega^n$. Let $f \in \mathcal{Y}$. Since $\mathcal{U} = k[X]$ is an unique factorization domain, we can factor f uniquely except for arrangement and units into irreducible polynomials: $f = P_1 \ldots P_r$. Now, $f \in \mathcal{Y} \implies$ there exists an irreducible non-constant polynomial $P \in \mathcal{Y}$. Since $\mathcal{U}$ is an unique factorization domain, it follows that $P \mathcal{U}$ is a prime ideal $\mathcal{Y}_0$. Let $\mathcal{Y}_0 \longrightarrow V_0$. From $\mathcal{Y}_0 \subseteq \mathcal{Y}$, we have $V_0 \supset V$, so $\dim V_0 \geq n-1$. However, $\mathcal{Y}_0 \neq (0)$, so $V_0 \neq \Omega^n$. Thus $\dim V_0 \leq n-1$. Hence, $\dim V_0 = n-1$, and $V_0 = V$, so $\mathcal{Y} = P\mathcal{U}$. Therefore, we see that any $n-1$ dimensional variety is defined by the zeros of a prime ideal which is generated by an irreducible non-constant polynomial.

Conversely, suppose we are given a non-constant irreducible polynomial P. Then $\mathcal{Y} = P\mathcal{U}$ is a prime ideal. Let V be the variety determined by $\mathcal{Y}$. Since $V \neq \Omega^n$, we have $\dim V \leq n-1$. To show that $\dim V = n-1$, all we must do is exhibit one point of V with this dimension. Since P is non-constant, it must depend on at least one variable - say X_n. Now select $x_1, \ldots, x_{n-1} \in \Omega$ algebraically independent, and solve in Ω:

$$P(x_1, x_2, \ldots, x_{n-1}, X_n) = 0.$$

Call the solution x_n. Then, by construction, $x = (x_1, x_2, \ldots, x_n)$ is a zero of P and, hence, a zero of $\mathcal{Y}$,

so $(x) \in V$, and, by construction, $\dim(x) = n-1$. Thus the variety determined by a prime ideal which is generated by an irreducible polynomial is of dimension $n-1$. We note that the prime ideal is unique up to a constant, i.e., if $P_1 \mathscr{r}$ and $P_2 \mathscr{r}$ (P_1, P_2 irreducible) give the same variety, then P_1 and P_2 differ by a constant. This fact is trivial to prove.

In the way of terminology, we call one dimensional varieties __curves__. Two dimensional varieties are called __surfaces__, and $n-1$ dimensional varieties are called __hypersurfaces__. We emphasize that an $n-2$ dimensional variety is not necessarily the intersection of two hypersurfaces. We will study in a later chapter the intersection of varieties in greater detail.

§4. __Products of algebraic sets__: In this short section, we want to introduce the concept of the product of two algebraic sets, and investigate a few of its properties.

Let $V \subset \Omega^n$, and $W \subset \Omega^m$ be algebraic sets. The set $V \times W \subset \Omega^{n+m}$, obtained by taking all points (x,y) such that $(x) \in V$ and $(y) \in W$, is called the __product__ of the algebraic sets V and W. We claim, first of all, that $V \times W$ is an algebraic set. For suppose $\mathscr{A} \longrightarrow V$ where $\mathscr{A}$ is an ideal of $k[X]$, and suppose $b \longrightarrow W$ where b is an ideal of $k[Y]$. Let $\mathscr{Y} = k[X,Y]$, and let $\mathscr{L} = \mathscr{A}\mathscr{Y} + b\mathscr{Y}$.

We show that the ideal $\mathcal{L}$ of $\mathcal{O}$ determines $V \times W$. Let (x,y) be a zero of $\mathcal{L}$; therefore, it must be a zero of $\mathcal{M}$. Thus (x) must be a zero of $\mathcal{M}$ since $\mathcal{M}$ doesn't depend on Y. Similarly, (y) is a zero of b, so any zero of $\mathcal{L}$ is of the form (x,y) where $(x) \in V$ and $(y) \in W$. Hence the zeros of $\mathcal{L}$ belong to $V \times W$. Conversely, if $(x,y) \in V \times W$, then clearly $\mathcal{L}(x,y) = 0$. Consequently, we get that $V \times W$ is an algebraic set defined by $\mathcal{L}$.

We observe the important fact that the product of two varieties is not necessarily a variety. To see this, consider the following example: let $k = Q$, the rational numbers, and let $\Omega = C$, the complex numbers. Consider the variety $V = \{(\sqrt{2}), (-\sqrt{2})\}$, i.e. the variety V consisting of the two points $(\sqrt{2})$ and $(-\sqrt{2})$. Then

$$V \times V = \{(\sqrt{2},\sqrt{2}), (-\sqrt{2},-\sqrt{2}), (\sqrt{2},-\sqrt{2}), (-\sqrt{2},\sqrt{2})\}$$

which splits into two varieties:

$$V \times V = \{(\sqrt{2},\sqrt{2}), (-\sqrt{2},-\sqrt{2})\} \cup \{(\sqrt{2},-\sqrt{2}), (-\sqrt{2},\sqrt{2})\}.$$

We have previously defined what we mean by the dimension of a variety. But we know that every algebraic set can be decomposed uniquely into a union of a finite number of component varieties. Hence, we define as the dimension of an algebraic set the maximal dimension of its component varieties, or, i.e., dimension of the algebraic set $V = \underset{(x) \in V}{\text{Max}} \dim(x)$. It is immediately clear

that the dimension of a proper algebraic subset of the
algebraic set V is not necessarily less than that of V.

Theorem 4.1: dim(V × W) = dim V + dim W.

Proof: Since dim(V × W) = Max dim(x,y),
                              (x)∈V
                              (y)∈W

it is clear that dim(V × W) ≤ dim V + dim W. Now choose
a point (x)∈ V with dim(x) = dim V, and choose a point
(y)∈ W with dim(y) = dim W, and such that the transcen-
dence base of (y) is algebraically independent of that
of (x). This can be done by the nature of Ω. Then
for this (x) and (y), we have dim(x,y) = dim V + dim W, so
dim(V × W) ≥ dim V + dim W, and the theorem follows.

Chapter II

Valuation Rings, Places, and Valuations

§1. <u>Introduction</u>: In Chapter I, we introduced some of
the basic concepts of algebraic geometry and obtained
several results using a minimum of algebraic tools. In
order to obtain deeper results, we will proceed in this
introductory section in developing the interconnection
between valuation rings, places, and valuations. Our
discussion will culminate in the extension theorem for
places which will be applied many times in the sequel to
get further results in algebraic geometry.

Let K be any field; we define, first of all, what is
meant by a valuation ring.

<u>Definition 1.1</u>: A subring $\mathscr{U}$ of K is called a valuation
ring if for any $a \in K$, $a \notin \mathscr{U} \implies a^{-1} \in \mathscr{U}$.

As an example of a valuation ring, we have, of
course, the entire field; we call this the <u>trivial
valuation ring</u>.

As an immediate consequence of the definition, we
have $1 \in \mathscr{U}$, so a valuation ring is a ring with an
identity element.

Let us now consider the set $\mathscr{U}$ of non-units of $\mathscr{U}$,
i.e.,

$$\mathscr{U} = \left\{ a \mid a \in \mathscr{U}, a^{-1} \notin \mathscr{U} \right\} .$$

It is immediately clear that the following statement holds:

(1.1) $\qquad a \notin \mathscr{S} \iff a^{-1} \in \mathscr{U}$.

  We investigate now some of the properties of $\mathscr{S}$.
We have:

1) If $a + b \notin \mathscr{S}$, then either a or b does not belong to $\mathscr{S}$.

Proof: The statement is certainly true if either a or b
is 0. Thus we assume that $a, b \neq 0$. Assume that $\frac{a}{b} \in \mathscr{U}$
(if $\frac{a}{b} \notin \mathscr{U}$, then $\frac{b}{a} \in \mathscr{U}$ and the argument is analogous).
Since $a + b \notin \mathscr{S}$, we have by (1.1) that $(a + b)^{-1} \in \mathscr{U}$.
Hence,

$$(1 + \tfrac{a}{b})(a + b)^{-1} \in \mathscr{U},$$

i.e., $b^{-1} \in \mathscr{U}$ whence $b \notin \mathscr{S}$, and the contention has been
established.

2) If $a, b \in \mathscr{U}$ and $ab \notin \mathscr{S}$, then neither a nor b belongs
to $\mathscr{S}$.

Proof: We have by hypothesis and (1.1) that $(ab)^{-1}b \in \mathscr{U}$,
so $a^{-1} \in \mathscr{U}$. Consequently, $a \notin \mathscr{S}$. In a similar manner,
we get $b \notin \mathscr{S}$.

  Taking the contrapositive statements of 1) and 2)
we have:

1') If a and b belong to $\mathscr{S}$, then $a + b \in \mathscr{S}$.

2') If $a, b \in \mathscr{U}$ and if either a or b belongs to $\mathscr{S}$,
then $ab \in \mathscr{S}$.

But 1') and 2') say that $\mathfrak{p}$ is an ideal. Thus the set of non-units of a valuation ring form an ideal. We also have that any ideal $\neq \mathcal{O}$ is contained in $\mathfrak{p}$, i.e., $\mathfrak{p}$ is the unique maximal ideal of $\mathcal{O}$, for any element of $\mathcal{O}$ not contained in $\mathfrak{p}$ is a unit. Therefore, $\mathcal{O}/\mathfrak{p}$ is a field; especially, $\mathfrak{p}$ is a prime ideal. Recapitulating, we have:

<u>Lemma 1.1</u>: The non-units, $\mathfrak{p}$, of a valuation ring $\mathcal{O}$ form a maximal ideal.

Let U denote the units of $\mathcal{O}$. Clearly, U is a multiplicative group. We now claim that the field K can be decomposed into the following <u>disjoint</u> union:

$$(1.2) \qquad K = \mathfrak{p} \cup U \cup \mathfrak{p}^{(-1)}$$

where $\mathfrak{p}^{(-1)}$ denotes the set of elements inverse to $\mathfrak{p}$ and where it is understood that we don't take the inverse of 0. Since $\mathfrak{p} \cup U = \mathcal{O}$, all we must show is that $\mathfrak{p}^{(-1)}$ consists of the complement of $\mathcal{O}$ in K. But this is clear, for if $a \notin \mathcal{O}$, then $a^{-1} \in \mathcal{O}$, but since $a^{-1} \notin U$, we have $a^{-1} \in \mathfrak{p}$, so $a \in \mathfrak{p}^{(-1)}$. While if $a \in \mathfrak{p}^{(-1)}$, then $a^{-1} \in \mathfrak{p}$, and $a \notin \mathcal{O}$. Thus (1.2) has been established. Also, we see that $\mathfrak{p}$ determines the valuation ring $\mathcal{O}$.

From (1.2), we get that if $\mathcal{O}_1$ and $\mathcal{O}_2$ are two valuation rings of K with non-units $\mathfrak{p}_1$, $\mathfrak{p}_2$ and units U_1, U_2, then

$$\mathcal{O}_1 \subset \mathcal{O}_2 \iff \mathfrak{p}_1 \supset \mathfrak{p}_2 \iff U_1 \subset U_2.$$

Next, we will introduce the concept of a place and show the relationship between it and a valuation ring.

Let K, F be two arbitrary fields.

__Definition 1.2:__ A map $\phi: K \longrightarrow F \cup \{\infty\}$ is called a place if:

1) $\phi^{-1}(F) = \mathscr{O}$ is a ring;

2) $\phi|\mathscr{O}$ is a non-trivial homomorphism;

3) if $\phi(a) = \infty$ (i.e., $a \notin \mathscr{O}$), then $\phi(a^{-1}) = 0$.

Before proceeding with some consequences, we give an example of a place. We take as K the field of rational functions in one variable, i.e., $F(x)$ where F is a field; write each element of $F(x)$ as a fraction in reduced form. Now substituting $x = a \in F$ gives a map of $F(x)$ into $F \cup \{\infty\}$ if we specify that if after substitution a 0 appears in the denominator, then we map this element into ∞. Clearly, the mapping is well-defined. Condition 1) is satisfied since if $f, g \in F(x)$ have denominators which are not divisible by $x - a$, then the same is true for their sum and product. On $\mathscr{O}$, the mapping is, of course, a homomorphism, and it is non-trivial since 1 does not go into 0. Condition 3) is obviously satisfied. Intuitively, therefore, we may view a place as a substitution.

As another example, we take $K = Q$, the field of rational numbers. We write each fraction so that not both numerator and denominator are divisible by some fixed

prime p   We now consider the map of Q into equivalence
classes obtained in the following manner: we replace
numerator and denominator by the residue class to which it
belongs modulo p. If the denominator is the 0 residue
class, we map the element into ∞. This map follows, of
course, the same procedure as the one of the first example
since for $f(x) \in F[x]$, we have $f(x) = (x-a)Q(x) + R$, and
$f(x) \equiv f(a) = R \mod(x-a)$.

    The first consequence we have from definition 1.2
is that $\mathscr{O} = \phi^{-1}(F)$ is a valuation ring. For if $a \notin \mathscr{O}$,
then $\phi(a) = \infty$ which implies by condition 3) that $\phi(a^{-1}) = 0$,
so $a^{-1} \in \mathscr{O}$. Now let us investigate the non-units $\mathscr{Y}$ of
the valuation ring $\mathscr{O} = \phi^{-1}(F)$. By (1.2), we know that
$\mathscr{Y}$ consists of 0 and the inverses of elements which do
not belong to $\mathscr{O}$. Thus we certainly have that $\phi(\mathscr{Y}) = 0$
(i.e., $\mathscr{Y}$ belongs to the Kernel of ϕ). Now suppose
$\phi(a) = 0$. If $a^{-1} \in \mathscr{O}$, then

$$\phi(aa^{-1}) = \phi(1) = \phi(a)\phi(a^{-1}) = 0,$$

so $\phi(1) = 0$ which implies that $\phi(\mathscr{O}) = 0$ and this contra-
dicts condition 2) of the definition. Hence, $a^{-1} \notin \mathscr{O}$,
so $\phi(a^{-1}) = \infty$, or $a^{-1} \in \mathscr{Y}^{(-1)}$. Thus $a \in \mathscr{Y}$. Consequently,
we have that $\mathscr{Y}$ is the kernel of ϕ on $\mathscr{O}$. The proof also
shows that $\phi(1) = 1$ (or this follows immediately from
condition 2)).

So far, we have associated with a place a valuation ring. Now let us start out with a valuation ring $\mathcal{O}$ given; we wish to associate with it a place ϕ. Let $\mathcal{Y}$ be the maximal ideal of non-units of $\mathcal{O}$. We define:

$$\phi(a) = \begin{cases} \infty & \text{if } a \notin \mathcal{O} \\ \\ a + \mathcal{Y} & \text{if } a \in \mathcal{O} . \end{cases}$$

That is, for $a \in \mathcal{O}$ we take the canonical map, so $F = \mathcal{O}/\mathcal{Y}$. Let us verify that this ϕ is indeed a place. By definition $\phi^{-1}(F) = \mathcal{O}$, the given valuation ring, so condition 1) is surely satisfied. $\phi|\mathcal{O}$ is, of course, a homomorphism, and it is non-trivial since $1 \notin \mathcal{Y}$. If $a \notin \mathcal{O}$, then $a^{-1} \in \mathcal{Y}$ by (1.2), so condition 3) is satisfied. Hence, ϕ is a place, and the ring belonging to this place is the given valuation ring.

Let us investigate more thoroughly the maps involved when a place ϕ is given: $\phi : K \longrightarrow F \cup \{\infty\}$. $\phi|\mathcal{O} : \mathcal{O} \longrightarrow F$ is a homomorphism with kernel $\mathcal{Y}$, as we've seen, so $\mathcal{O}/\mathcal{Y} \simeq \phi(\mathcal{O})$. Therefore, we have the following sequence of maps:

$$\mathcal{O} \xrightarrow{\ \kappa\ } \mathcal{O}/\mathcal{Y} \xrightarrow{\ j\ } \phi(\mathcal{O}) \xrightarrow{\ i\ } F.$$

The map κ is the canonical map, j is an isomorphism, and i is the injection map. However, the map χ (where χ takes a $\notin \mathcal{O}$ into ∞) is the place we would have gotten if we had started with the valuation ring $\mathcal{O}$ as given.

Thus we have, summarizing the preceding discussion, that places and valuation rings are in a one-to-one correspondence provided we have the following understanding: a given place determines a valuation ring which in turn determines the given place up to isomorphism. We will say that two places are <u>equivalent</u> if they have the same valuation ring. Hence, there is a one-to-one correspondence between places and valuation rings up to an equivalency.

Next, we want to connect the concepts of place and valuation ring with that of a valuation. Before defining what is meant by a valuation, we must define what we mean by an ordered group. Let G be a group written multiplicatively.

<u>Definition 1.3</u>: The group G is said to be ordered if G contains an invariant sub-semigroup S such that

$$G = S \cup \{1\} \cup S^{(-1)}$$

(where the union is meant to be disjoint).

Now we show that this definition leads to a sensible ordering, i.e., the usual conditions of ordering are satisfied. Namely, we define for a, b $\in$ G where G is an ordered group: a < b if and only if $ab^{-1} \in$ S (so a < 1 $\iff$ a $\in$ S).
a) We first note: a < b $\iff$ $ab^{-1} \in$ S $\iff$ $b^{-1}a \in$ S.
<u>Proof</u>: Since $b^{-1}a = b^{-1}(ab^{-1})b$, if $ab^{-1} \in$ S, then $b^{-1}a \in$ S by the invariance of S, and since $ab^{-1} = b(b^{-1}a)b^{-1}$, we get the implication the other way.

Now, we have from the decomposition of G that either
1) $ab^{-1} \in S$, or 2) $ab^{-1} \in \{1\}$, or 3) $ab^{-1} \in S^{(-1)}$.
That is, either 1) $a < b$, or 2) $a = b$, or 3) $b < a$.

b) $a < b$, $b < c \longrightarrow a < c$. Since we have $ab^{-1} \in S$ and $bc^{-1} \in S$ by the semigroup property of S, we get $ac^{-1} \in S$, so $a < c$.

c) $a < b \longrightarrow ac < bc$. For $ab^{-1} \in S$, so $acc^{-1}b^{-1} \in S$, i.e. $ac < bc$. Similarly, we show $ca < cb$.

d) $a < b \longrightarrow b^{-1} < a^{-1}$. From $a < b$, we get, applying c), that $1 < a^{-1}b$, and, by another application of c), we get $b^{-1} < a^{-1}$.

e) $a < b$, $c < d \Longrightarrow ac < bd$. Since $a < b$, using c), we get $ac < bc$. Similarly, we have $bc < bd$. Then, using b), we get $ac < bd$.

If G should be a commutative group, we can, of course, omit the word invariant in definition 1.3. It is also possible that there is an addition defined in G. However, if not, we can always define one for an ordered group. We simply take: $a + b = \text{Max}(a,b)$. That this is well-defined follows from the discussion after the proof of a). It is clearly an associative operation. Let us show that it is distributive, i.e., we claim that $(a + b)c = ac + bc$. Suppose that $a \leq b$ (i.e., either $a < b$ or $a = b$), then $ac \leq bc$, and $\text{Max}(ac,bc) = bc$; while $\text{Max}(a,b) \cdot c = bc$.

To the ordered group G, we will adjoin a zero element, 0, such that multiplying any element of G by 0 yields 0

and such that 0 is less than every element of G in the
ordering. Then a + 0 = 0 + a = a for any a $\in$ G.

Finally, we can define what is meant by a valuation
of a field K.

Definition 1.4: A valuation of a field K is a map | |:
K $\longrightarrow$ G $\cup$ {0} where G is an ordered group, and where | |
is such that:

1) $|a| = 0 \iff a = 0$

2) $|ab| = |a||b|$

3) $|a + b| \leq |a| + |b|$.

As an immediate consequence, we have that $|1| = 1$.
Also, $|-1| = 1$; since from condition 2) we get $|-1|^2 = |1| = 1$,
but in an ordered group we can't have an element $\neq 1$ of
finite period, for if, say, a > 1, then all powers of a
are greater than 1.

Now, if in G the addition is based on the Max, we
will show that from a valuation we get a valuation ring.
Let

$$\mathcal{O} = \left\{ a \mid a \in K, \ |a| \leq 1 \right\} .$$

First, we show that $\mathcal{O}$ is a ring. If $|a| \leq 1$ and $|b| \leq 1$,
then $|ab| = |a||b| \leq 1$, and $|a + b| \leq \text{Max}(|a|,|b|) \leq 1$.
Next, we show that $\mathcal{O}$ is a valuation ring. If a $\notin \mathcal{O}$, then
$|a| > 1$, so $|a^{-1}| = |a|^{-1} < 1$. Thus $a^{-1} \in \mathcal{O}$, so $\mathcal{O}$ is
a valuation ring. The non-units $\mathcal{U}$ of $\mathcal{O}$ are those a $\in \mathcal{O}$
such that $a^{-1} \notin \mathcal{O}$, i.e., those a such that $|a| \leq 1$, and

$|a|^{-1} > 1$, so

$$\mathcal{Y} = \left\{ a \,\middle|\, |a| < 1 \right\} \;,$$

and, consequently, the units of $\mathcal{U}$ are

$$U = \left\{ a \,\middle|\, |a| = 1 \right\} \;.$$

Let us analyze the map $|\;|$ more carefully. Let $K^* = K - \left\{ 0 \right\}$; then by condition 2) the map

$$|\;| \colon K^* \longrightarrow G$$

is a homomorphism, and, as we've seen, the kernel is U; therefore $K^*/U \simeq |K^*|$ where $|K^*|$ denotes the image of K^* under $|\;|$. Thus we have the following sequence of maps

$$K^* \longrightarrow K^*/U \overset{j}{\longrightarrow} |K^*| \overset{i}{\longrightarrow} G$$

where j is an isomorphism, and i is the injection map.

Now let us suppose that we are given a valuation ring $\mathcal{U}$ belonging to a field K; $\mathcal{Y}$ its maximal ideal, and U the group of units. We wish to obtain a valuation. From the above discussion, we see that we should define for $a \in K$: $|a| = aU$. The set of all $\left\{ aU \right\}$ form $K^*/U \cup \left\{ 0 \right\}$. We must, first of all, show that the group $G = K^*/U$ is ordered. To do this, we must exhibit a sub-semi group S with the required properties. We define S in the following way: $aU \in S$ if and only if $aU \subset \mathcal{Y}$, i.e., if and only if $a \in \mathcal{Y}$. Clearly, S is a semi group, and, of course, invariant since K is a field. Since

$$K^* = (\mathcal{Y} - \{0\}) \cup U \cup (\mathcal{Y} - \{0\})^{(-1)} \quad \text{(disjoint)},$$

we get mod U that

$$G = K^*/U = S \cup \{1\} \cup S^{(-1)} \quad \text{(disjoint)},$$

so, indeed, K^*/U is an ordered group.

How let us check that $|a| = aU$ satisfies the other conditions for a valuation. The first two conditions are immediate. To verify condition 3), we must show that $|a + b| \leq |a| + |b|$. However, this is equivalent to the following: $|a| \leq 1 \implies |1 + a| \leq 1 + |a|$. For, say, $|\frac{a}{b}| \leq 1$, then $|1 + \frac{a}{b}| \leq 1 + |\frac{a}{b}|$, so $|a + b| \leq |a| + |b|$; the implication the other way is trivial. Thus in our case, i.e., with addition based on the max, all we must show is that $|a| \leq 1 \implies |1 + a| \leq 1$. Hence, suppose that $aU = |a| \leq 1$. This implies that $a \in \mathcal{U}$. Thus $1 + a \in \mathcal{U}$, so $|1 + a| \leq 1$. Therefore, $|a| = aU$ is a valuation, and, moreover, its associated valuation ring is the given one $\mathcal{U}$.

Summarizing, we have that there is a one-to-one correspondence between valuations and valuation rings with the understanding that a given valuation determines a valuation ring which, in turn, determines the given valuation up to isomorphism. Since we have already seen that there is a one-to-one correspondence between places and valuation rings with the usual understanding, we now have the complete interconnection of the three concepts.

Before proceeding further with the theory, we will illustrate the preceding discussion by means of an example. Let $K = C(z)$ be the field of rational functions of a single complex variable. We know that a place is obtained by substituting z_0 for z. The valuation ring of this place is

$$\mathscr{J} = \left\{ \frac{f(z)}{g(z)} \;\middle|\; g(z_0) \neq 0 \right\}$$

where $f, g \in C[z]$; while the maximal ideal of non-units is

$$\mathscr{Y} = \left\{ \frac{f(z)}{g(z)} \;\middle|\; g(z_0) \neq 0, \; f(z_0) = 0 \right\},$$

and the group of units is

$$U = \left\{ \frac{f(z)}{g(z)} \;\middle|\; g(z_0) \neq 0, \; f(z_0) \neq 0 \right\}.$$

The valuation associated with this valuation ring is $|f(z)| = f(z)U$ where $f(z) \in C(z)$. Hence, $|f(z)| = (z - z_0)^n U$. n is called the order of the zero of $f(z)$ at z_0 where a negative n is counted as a pole, and where $n = 0$ means that $f(z)$ has no zero or pole at z_0. We see that the ordered group G is simply a cyclic group generated by $(z - z_0)U$ and is isomorphic to Z, the additive group of integers. We also have

$$|f(z)| < 1 \iff (z - z_0)^n \in \mathscr{Y} \iff n > 0,$$

and we can see that G has the reverse ordering of Z.

Summarizing, we see that the place merely tells us whether a function approaches 0 or ∞ at a particular point, whereas the valuation gives us a refinement of this statement by telling us with what order the function goes to 0 or ∞.

Now, let us return to the general theory. We want to prove the fundamental theorem on the extension of a homomorphism to a place. This theorem will play a fundamental role in our development of algebraic geometry.

Theorem 1.1: Let K be any field and $\mathcal{O}$ a subring of K. Let F be an algebraically closed field; suppose $f: \mathcal{O} \longrightarrow F$ is a non-trivial homomorphism. Then there exists a place ϕ of K such that $\phi|\mathcal{O} = f$ (note: ϕ is not necessarily unique).

Proof: There are two types of extensions that we will consider. We proceed to describe the first of these. Let S consist of those elements $s \in \mathcal{O}$ such that $f(s) \neq 0$. Clearly, S forms a semi-group, and $S \neq \emptyset$ since f is non-trivial. In general, given a commutative ring R and a sub-semi group S which contains no divisors of zero, we can form the quotient ring consisting of all $\frac{r}{s}$, $r \in R$, $s \in S$.[*] In our case, we form

$$\mathcal{O}' = \left\{ \frac{a}{s} \,\middle|\, a \in \mathcal{O}, \; s \in S \right\} .$$

$\mathcal{O}'$ is a ring with an identity element. We extend f to f' on $\mathcal{O}'$ by defining

$$f'\left(\frac{a}{s}\right) = \frac{f(a)}{f(s)} .$$

---

[*] See N. H. McCoy, *Rings and Ideals*, Carus Mathematical Monographs, p. 94.

Let us show that f' is well-defined. If $\dfrac{a_1}{s_1} = \dfrac{a_2}{s_2}$, then $a_1 s_2 = a_2 s_1$, and, since f is a well-defined homomorphism, we have $f(a_1)f(s_2) = f(a_2)f(s_1)$. But $f(s_1) \neq 0$, and $f(s_2) \neq 0$, so dividing, we get

$$\frac{f(a_1)}{f(s_1)} = \frac{f(a_2)}{f(s_2)}$$

which establishes that f' is well-defined. It is clear that f' is a homomorphism since f is. Finally $f'|\mathscr{U} = f$, for if $a \in \mathscr{U}$, then we can write it as $\dfrac{as}{s}$, and

$$f'(\frac{as}{s}) = \frac{f(a)f(s)}{f(s)} = f(a).$$

Therefore, we have that f' is an extension of f.

This is the first type of extension, but it may yield no extension at all; this happens when the ring $\mathscr{U}$ is its own quotient ring, i.e., when for any $a \in \mathscr{U}$ if $f(a) \neq 0$, then $a^{-1} \in \mathscr{U}$. When this happens, we will show that if we select any $a \in K$, we can extend f to either $\mathscr{U}[a]$ or to $\mathscr{U}[a^{-1}]$,- the second type of extension. First, we observe that if $f(\mathscr{U}) = F_0 \subset F$, then F_0 is a field, for let $s_0 \in F_0$, and $s_0 \neq 0$. Then $s_0 = f(a) \neq 0$ for some $a \in \mathscr{U}$; hence, $a^{-1} \in \mathscr{U}$, and $1 = f(aa^{-1}) = f(a)f(a^{-1}) = s_0 f(a^{-1})$.

Let $\bar{a}$ denote the image of $a \in \mathscr{U}$ under f. Extend f to $\mathscr{U}[X]$ in the obvious manner (i.e. just apply f to the coefficients of a polynomial of $\mathscr{U}[X]$; strictly speaking, we should use a new variable Y in this map, but we won't do this in order to avoid introducing too much notation).

The image of $P(X) \in \mathscr{A}[X]$ will be denoted by $\bar{P}(X)$. The image of $\mathscr{A}[X]$ is, of course, $F_0[X]$ where $F_0[X]$ is a principal ideal domain. Now, we attempt to extend f to g on $\mathscr{A}[a]$ by defining $g(P(a)) = \bar{P}(\xi)$ where ξ is any element of F. If g is well-defined, it is clearly a homomorphism and is an extension of f. So, we must just see if it is well-defined: i.e., does $P(a) = 0 \longrightarrow \bar{P}(\xi) = 0$?

Consider the set $\mathscr{M}$ of all $P(\lambda)$ with $P(a) = 0$. It is the kernel of the substitution map: $\mathscr{A}[X] \longrightarrow \mathscr{A}[a]$. $\mathscr{M}$ is, of course, an ideal of $\mathscr{A}[X]$, so our question as to whether g is well-defined can be worded as follows: Is the image $\overline{\mathscr{M}}$ in $F_0[X]$ of $\mathscr{M}$ of such a nature that $X = \xi$ is a zero of it? Since $\overline{\mathscr{M}}$ is an ideal of the principal ideal domain $F_0[X]$, we have: $\overline{\mathscr{M}} = \bar{Q}(X) \cdot F_0[X]$. Thus ξ must be selected as a zero of $\bar{Q}(X)$, and, since F is algebraically closed, such a ξ can be chosen, provided $\bar{Q}(X) \neq$ a non-zero constant, and we have an extension to $\mathscr{A}[a]$. But it is possible that $\bar{Q}(X)$ is a non-zero constant (if $\bar{Q}(X) = 0$, then any $\xi \in F$ works) in which case our construction does not work, so we must consider in detail this case. We may assume that $\bar{Q}(X) = 1$. Then there is a

$$Q(X) = 1 + p_0 + p_1 X + \dots + p_r X^r$$

where $\bar{p}_i = 0$, $i = 0, \dots, r$, and where

$$1 + p_0 + p_1 a + \dots + p_r a^r = 0.$$

Thus if a satisfies such an equation, our attempted construction doesn't go through. However, we now show that the attempt can't fail with both a and $a^{-1} = \beta$. For suppose it did. Then a, β satisfy

(1.3) $1 + p_o + p_1 a + \ldots + p_r a^r = 0$

(1.4) $1 + p'_o + p'_1 \beta + \ldots + p'_s \beta^s = 0$

where $\bar{p}_i = \bar{p}'_j = 0$, $i = 0, \ldots, r$; $j = 0, \ldots, s$, and where we may assume that r and s are minimal. We note that r and s are greater than or equal 1, for if, for example, $r = 0$, then $1 + p_o = 0 \implies I + \bar{p}_o = 0$, or $I = 0$ which is a contradiction. We may assume that $s \leq r$ since the argument will be symmetric in r and s. Since $\beta = a^{-1}$, we have from (1.4)

$$a^s = -\frac{p'_1}{1+p'_o} \, a^{s-1} - \ldots - \frac{p'_s}{1+p'_o} \, ,$$

or

(1.5) $a^s = p''_o + p''_1 a + \ldots + p''_{s-1} a^{s-1}$

where $p''_i \in \mathcal{U}$ since $I + \bar{p}'_i = I \neq 0$, and where $\bar{p}''_i = 0$ $i = 0, \ldots, s-1$. Since $s \leq r$, we can write

$$a^r = a^s(a^{r-s}) \, ;$$

therefore, we can, using (1.5), lower the degree of a in (1.3); i.e., we have

$$1 + p_o + p_1 a + \ldots + p_r(a^{r-s})a^s = 0,$$

or

48.

(1.6) $1 + p_0 + p_1 a + \ldots + p_r a^{r-s}(p_0'' + \ldots + p_{s-1}'' a^{s-1}) = 0,$

and the highest power of a in (1.6) is $r-1$ which contradicts the minimal character of r. Hence, if we can't extend f to $\mathscr{O}[a]$, then we can extend it to $\mathscr{O}[a^{-1}]$.

Now, we are in a position to apply Zorn's Lemma.[*] Consider the set E of all extensions of f to larger rings. If g_1, g_2 are two such extensions, we say that $g_2 > g_1$ if g_2 is an extension of g_1 (i.e. the ring on which g_2 is defined contains the ring on which g_1 is defined and g_2 restricted to the ring of g_1 is equal g_1). Clearly, this yields a partial ordering of E. We must show that every totally ordered subset of E has an upper bound. Let $\{g_\alpha\}$ be a totally ordered subset of E; the rings on which the g_α are defined are ordered by inclusion. Take the union of these rings and consider the map g defined on this union as follows: if $\gamma \in$ the union, then $\gamma \in$ some set of the union, and g should act on γ as the original g_α did. The definition is consistent since all $g_\beta > g_\alpha$ are extensions of g_α, and g is a homomorphism since if $\gamma_1, \gamma_2 \in$ union; then $\gamma_1, \gamma_2 \in$ some set of the union since the rings are ordered by inclusion, so the statement is clear. Also, it is clear that g is an extension of any g_α, and is an upper bound. Thus E is inductively ordered in the sense

of Bourbaki, so by Zorn's Lemma E has a maximal element.
Let g be such a maximal element: $g: \mathcal{U} \longrightarrow F$. Since g
cannot be extended any further, we know by the preceding
discussion that: 1) $\mathcal{U}$ is its own quotient ring by elements
with non-zero images, i.e., if $a \in \mathcal{U}$, and if $g(a) \neq 0$,
then $a^{-1} \in \mathcal{U}$.

2) If $a \notin \mathcal{U}$, then we know that we cannot extend g to
$\mathcal{U}[a]$ since g is maximal, but, as we know, this implies
that we can extend g to $\mathcal{U}[a^{-1}]$. Hence, we must have
$a^{-1} \in \mathcal{U}$ since g is maximal, so if $a \notin \mathcal{U}$, then $a^{-1} \in \mathcal{U}$,
i.e., $\mathcal{U}$ is a valuation ring.

Now, we must show that the place ϕ belonging to this
valuation ring is g up to isomorphism. This follows from
1) since $g(a) \neq 0 \Longleftrightarrow a^{-1} \in \mathcal{U}$, so the kernel $\mathcal{U}$ of g
is the set of non-units of $\mathcal{U}$. Now, extend g to K
by mapping a into ∞ if $a \notin \mathcal{U}$, and g equals ϕ up to
isomorphism, and the proof of the extension theorem is
completed

§2. <u>Applications to algebraic geometry</u>: We want now to
apply the extension theorem of places to get further results
in algebraic geometry. We contend:
<u>Contention</u>: Let $(x) \in \Omega^n$, and $f(X) \in k[X]$, and suppose
that $f(x) \neq 0$; then there exists an algebraic specialization
$(x) \longrightarrow (x_0)$ (i.e., all components of (x_0) are algebraic)
such that $f(x_0) \neq 0$.

<u>Proof:</u> If $(x) = (x_1, x_2, \ldots, x_n)$ is algebraic, then we simply take $(x_0) = (x)$, and we are done. Thus, suppose that $x_1, \ldots, x_r$ are algebraically independent over k while all other x_i are algebraic over $k(x_1, \ldots, x_r)$. Let a designate any of the x_i or $\frac{1}{f(x)}$; then a is algebraic over $k(x_1, \ldots, x_r)$. Hence, there exist equations of the form:

$$(2.1) \quad a_{0,a}(x_1, \ldots, x_r) a^{j_a} + \ldots + a_{s,a}(x_1, \ldots, x_r) = 0,$$

i.e., for each different a we have an equation of this type where the coefficients are in $k[x_1, \ldots, x_r]$. Now choose $x_1^0, \ldots, x_r^0$ from the algebraic closure of k in Ω in such a way that $a_{0,a}(x_1^0, \ldots, x_r^0) \neq 0$ for all a considered. Let us show that such a choice is possible. It is clear, by taking the product of all $a_{0,a}(x_1, \ldots, x_r)$, that we need consider only a single polynomial; also, we observe that we wish to choose elements from the algebraic closure which is an infinite field. Thus our problem reduces to the following: If a non-zero polynomial in several variables is given with coefficients in an infinite field can we choose values from this field such that the polynomial remains non-zero upon substitution of these values? We prove that such a choice is possible by induction on the number of variables. The choice is trivial if there are no variables. Suppose such a choice is possible if the polynomial contains n-1 variables. Consider now a non-zero polynomial of n

variables. Write the polynomial as one in terms of the n-th variable whose coefficients are polynomials in the other n-1 variables; not all these coefficients are 0, for then the given polynomial would also be 0. By induction, we can choose values in the field so that after substitution at least one of these coefficients is not zero. Making this substitution, we get a non-zero polynomial in one variable which has at most as many roots in the field as its degree. Since the field is infinite, we can choose a value such that the polynomial remains non-zero upon substitution, and the proof that such a choice of $x_1^0,\ldots,x_r^0$ is possible is completed.

Now let f be the substitution map:

$$f: k[x_1,\ldots,x_r] \longrightarrow \Omega$$

given by mapping $x_i \longrightarrow x_i^0$, $i = 1,\ldots,r$. Since $x_1,\ldots,x_r$ are algebraically independent, the map is well-defined and, consequently, a homomorphism. Now extend this homomorphism to a place ϕ of the field $k(x_1,\ldots,x_n)$, i.e.,

$$\phi: k(x_1,\ldots,x_n) \longrightarrow \Omega \cup \{\infty\}.$$

Clearly, ϕ is identity on k and $\phi(x_i) = x_i^0, i = 1,\ldots,r$. Put $\phi(x_i) = x_i^0$, $i = r + 1,\ldots,n$, so $\phi(x_i) = x_i^0$, for $i = 1,\ldots,n$. We claim that $\phi(a) \neq \infty$ for any a. For suppose that $\phi(a) = \infty$; then $\phi(\frac{1}{a}) = 0$. From (2.1), we have

$$(2.2) \quad a_{0,a}(x_1,\ldots,x_r) + a_{1,a}(x_1,\ldots,x_r)\frac{1}{a} + \ldots +$$

$$a_{s,a}(x_1,\ldots,x_r)\frac{1}{a_a^{j_a}} = 0,$$

and, applying ϕ, we get

$$a_{0,a}(x_1^0, \ldots, x_r^0) = 0$$

which contradicts the choice of $x_1^0, \ldots, x_r^0$. Therefore, $\phi(a) \in \Omega$ for all a, and, applying ϕ to (2.1), we see that $\phi(a)$ is algebraic over $k(x_1^0, \ldots, x_r^0)$, and, therefore, $\phi(a)$ is algebraic over k. Thus, $(x_0) = (x_1^0, \ldots, x_n^0)$ is algebraic, and $(x) \longrightarrow (x_0)$ is a specialization since ϕ is a homomorphism on $\phi^{-1}(\Omega)$. Finally, we have that $\phi(f(x)) = f(x^0)$ is finite, and $\neq 0$ since $\phi(a) \neq \infty$ for any a. Hence, the contention has been completely established.

From the contention, we o tain immediately the following theorem:

Theorem 2.1: Let V be an algebraic set of Ω^n and V_0 the subset of algebraic points of V. Let $f \in k[X]$ be such that $f(V_0) = 0$ (i.e. f vanishes on all of V_0), then $f(V) = 0$.

Proof: Suppose $(x) \in V$, and $f(x) \neq 0$; then, by the contention, there exists an algebraic specialization $(x) \longrightarrow (x_0) \in V$ such that $f(x_0) \neq 0$, but this is a contradiction.

Before proceeding further, we must develop a little more algebraic "background" material. Let $\mathcal{O}$ be any ring (not necessarily containing an identity element), and let S be a multiplicative semi-group contained in $\mathcal{O}$. Suppose that $\mathcal{M}$ is an ideal of $\mathcal{O}$ such that $\mathcal{M} \cap S = \phi$ (note:

this implies that $0 \notin S$). Now consider the set Σ of all ideals containing $\mathfrak{M}$ which do not intersect S. Σ is partially ordered by inclusion, and for any totally ordered subset of Σ, the union is an ideal which does not intersect S. Consequently, Σ is inductively ordered and, by Zorn's Lemma, contains at least one maximal element $\mathscr{Y}$. Clearly, any ideal containing $\mathscr{Y}$ will intersect S. We wish to show that $\mathscr{Y}$ is a prime ideal. Suppose $a, b \notin \mathscr{Y}$; we must show that $ab \notin \mathscr{Y}$. Suppose, on the contrary, that $ab \in \mathscr{Y}$. Let $(a, \mathscr{Y})$ and $(b, \mathscr{Y})$ be the ideals generated respectively by a and $\mathscr{Y}$ and by b and $\mathscr{Y}$. They meet the semi-group S in elements s_1 and s_2.

$$s_1 = \pi_1 + m_1 a + x_1 a,$$

and

$$s_2 = \pi_2 + m_2 b + x_2 b$$

where $\pi_1, \pi_2 \in \mathscr{Y}$; m_1, m_2 are integers and $x_1, x_2 \in \mathscr{O}$. Then

$$s_1 s_2 = \pi_1 s_2 + (m_1 a + x_1 a) \pi_2 + (m_1 a + x_1 a)(m_2 b + x_2 b).$$

This shows that if $ab \in \mathscr{Y}$, then $s_1 s_2 \in \mathscr{Y}$, so $\mathscr{Y}$ meets S which is a contradiction.

We note, first of all, that if $\mathscr{O}$ is Noetherian, then we don't have to employ Zorn's Lemma for the existence of $\mathscr{Y}$. Secondly, we observe that if $\mathscr{O}$ contains an identity element, we get the existence of maximal ideals for $\mathscr{O}$ by taking $S = \{1\}$.

Now let $\mathcal{M}$ be any ideal of $\mathcal{V}$. Suppose $b \in \mathcal{V}$ has the property that $b^{\nu} \notin \mathcal{M}$ for any positive integer ν (hence, $b \neq 0$). Take $S = \{b^{\nu}$, where ν ranges over the positive integers$\}$. Then, as we've seen, there exists a prime ideal $\mathcal{Y} \supset \mathcal{M}$ such that $b^{\nu} \notin \mathcal{Y}$ for any positive integer ν. Let $\bar{\mathcal{a}} = \bigcap_{\mathcal{Y} \supset \mathcal{M}} \mathcal{Y}$ (where the $\mathcal{Y}$ designate prime ideals). $\bar{\mathcal{M}}$ is, of course, an ideal, and $b \notin \bar{\mathcal{M}}$ since, by the above, there exists a $\mathcal{Y} \supset \mathcal{M}$, and $b \notin \mathcal{Y}$. Thus $b \in \bar{\mathcal{M}} \Longrightarrow b^{\nu} \in \mathcal{M}$ for some positive integer ν. Suppose, conversely, that b has the property that some $b^{\nu} \in \mathcal{M}$. If $\mathcal{Y}$ is any prime ideal such that $\mathcal{Y} \supset \mathcal{M}$, then $b^{\nu} \in \mathcal{Y}$, so $b \in \mathcal{Y}$; hence, $b \in \bar{\mathcal{M}}$. Therefore, we have established that

$$\bar{\mathcal{M}} = \left\{ b \,\middle|\, b \in \mathcal{V} \text{ and } b^{\nu} \in \mathcal{M} \text{ for some } \nu \right\}.$$

The ideal $\bar{\mathcal{M}}$ is called the <u>radical</u> of the ideal $\mathcal{M}$. If $\mathcal{M} = (0)$, then we see that its radical $\bar{\mathcal{M}}$ consists of the totality of nilpotent elements of $\mathcal{V}$ - called the radical of the ring.

Now consider the set F of all prime ideals containing $\mathcal{M}$. This set is partially ordered under reverse inclusion. Consider any totally ordered subset $\{\mathcal{Y}_a\}$ of F. Let $\mathcal{Y}_0 = \bigcap_a \mathcal{Y}_a$; we must show that $\mathcal{Y}_0$ is a prime ideal. Let $ab \in \mathcal{Y}_0$, and $a \notin \mathcal{Y}_0$. Then $a \notin$ some $\mathcal{Y}_a \Longrightarrow a \notin \mathcal{Y}_\beta \subset \mathcal{Y}_a$, but $ab \in$ every $\mathcal{Y}_\beta$, so $b \in \mathcal{Y}_\beta$ for all $\mathcal{Y}_\beta \subset \mathcal{Y}_a$. Thus $b \in \mathcal{Y}_0$, so $\mathcal{Y}_0$ is a prime ideal;

consequently, the totally ordered set $\{\mathcal{P}_a\}$ has a lower bound whence F is inductively ordered. Therefore, there exists a minimal element in the set F, i.e., among the primes containing $\mathcal{M}$, there are certain minimal ones, and all others contain one of these. Thus we see that it suffices in the definition of the radical $\overline{\mathcal{M}}$ to take only the minimal prime ideals containing $\mathcal{M}$. Hence:

Theorem 2.2: The radical of an ideal $\mathcal{M}$ in the ring $\mathcal{O}$ is the intersection of all minimal prime ideals containing $\mathcal{M}$.

We also observe that our previous procedure gives us the existence of minimal prime ideals of $\mathcal{O}$ by taking $\mathcal{M} = (0)$.

Now, we are ready to return to the discussion of algebraic geometry. As usual, we let $\mathcal{O} = k[X]$, and let $\mathcal{M}$ be an ideal of $\mathcal{O}$ which determines the algebraic set V.

We contend: $\overline{\mathcal{M}}$, the radical of $\mathcal{M}$, is the ideal determined by V. For let $V \longrightarrow \widetilde{\mathcal{M}}$, i.e.,

$$\widetilde{\mathcal{M}} = \left\{ f \mid f \in \mathcal{O}, \ f(V) = 0 \right\}.$$

Let $\mathcal{P}$ be any prime ideal containing $\mathcal{M}$; then $\mathcal{P} \longrightarrow W$, a variety, and $W \subset V$. But $W \subset V \Longrightarrow \mathcal{P} \supset \widetilde{\mathcal{M}}$, so $\bigcap_{\mathcal{P} \supset \mathcal{M}} \mathcal{P} \supset \widetilde{\mathcal{M}}$, i.e., $\overline{\mathcal{M}} \supset \widetilde{\mathcal{M}}$. However, if $f \in \overline{\mathcal{M}}$, then $f^n \in \mathcal{M}$ for some n; hence, $f^n(V) = 0 \Longrightarrow f(V) = 0 \Longrightarrow f \in \widetilde{\mathcal{M}}$, so $\overline{\mathcal{M}} \subset \widetilde{\mathcal{M}}$. Combining the two results, we get $\overline{\mathcal{M}} = \widetilde{\mathcal{M}}$, and the contention is established.

We know that the radical of $\mathcal{M}$ can be given, for a general ring $\mathcal{O}$, by $\left\{ f \mid f \in \mathcal{O}, \ f^v \in \mathcal{M} \text{ for some } v \right\}$. We now ask whether there is a limit to the power one must take. The answer is yes when $\mathcal{O}$ is Noetherian; in particular, when $\mathcal{O} = k[X]$. To see this, write

$$\overline{\mathcal{M}} = f_1 \mathcal{O} + \ldots + f_r \mathcal{O}$$

where $f_1^{n_1} \in \mathcal{M}$. Let f be any element of $\overline{\mathcal{M}}$; then

$$f = f_1 g_1 + \ldots + f_r g_r$$

where the $g_1 \in \mathcal{O}$, and

$$f^{n_1 + \ldots + n_r} = (f_1 g_1 + \ldots + f_r g_r)^{n_1 + \ldots + n_r} \in \mathcal{M}.$$

Now, let $\mathcal{M}$ be an ideal and V its algebraic set, and let V_o be the algebraic points of V. Then we saw, by Theorem 2.1, that $f(V_o) = 0 \implies f(V) = 0$, but this implies, by the previous contention, that $f \in \overline{\mathcal{M}}$, the radical of $\mathcal{M}$, i.e., $f^n \in \mathcal{M}$ for some positive integer n. Thus we have established:

Theorem 2.3: <u>Hilbert's Nullstellensatz</u> (strong form): Let $\mathcal{M}$ be an ideal of the ring $\mathcal{O} = k[X]$; suppose $\mathcal{M} \longrightarrow V$, and V_o, the subset of algebraic points of V. If $f \in \mathcal{O}$ is not identically zero and is such that $f(V_o) = 0$, then $f^n \in \mathcal{M}$ for some positive integer n.

Thus we see that we can almost characterize the polynomials of the ideal $\mathcal{M}$ by just knowing V_o. If $\mathcal{M} = \mathcal{H}$,

a prime ideal, then the algebraic points characterize the ideal, for if $f(V_0) = 0$, then $f^n \in \mathscr{Y} \implies f \in \mathscr{A}$.

We also can reconcile now the two points of view concerning whether the components of a zero of an ideal of $\mathscr{A}$ are taken from just an algebraically closed field or from a field Ω of the type we have been considering. For let $V_0 \longrightarrow b$; by the Hilbert Nullstellensatz, we have $b \subset \overline{\mathscr{M}}$ where $\mathscr{M} \longrightarrow V$, but since $V_0 \subset V$, we have $b \supset \overline{\mathscr{M}}$, so $b = \overline{\mathscr{M}}$. Consequently, we have $V_0 \longrightarrow \overline{\mathscr{M}} \longrightarrow V$, i.e, the algebraic set is already characterized if we know its algebraic points. Hence, if we started with an algebraically closed field, we could always enlarge it so as to accomodate V which is already characterized by V_0.

Finally, suppose that $V = \phi$; then $V_0 = \phi$. Therefore, it is vacuously true that all $f \in \mathscr{A}$ vanish on V_0 whence for all $f \in \mathscr{A}$, $f^n \in \mathscr{M}$ for some n. In particular, $1 \in \mathscr{M}$, so $\mathscr{M} = \mathscr{A}$. Thus, we have shown:

<u>Theorem 2.4</u>: <u>Hilbert's Nullstellensatz</u> (weak form): Let $\mathscr{M}$ be an ideal of the ring $\mathscr{A} = k[X]$; then $\mathscr{M}$ without zeros $\implies \mathscr{M} = \mathscr{A}$.

§3. <u>Integral Closure</u>: Let $\mathscr{A}$ be a ring (with identity, as usual), and let $\mathscr{A}$ be a subring of the field K. We will first define what is meant by the integral closure of $\mathscr{A}$ in K without using places; then we will show the interconnection of this concept with that of places.

Definition 3.1: An element $a \in K$ is called integral over $\mathcal{O}$ if a satisfies an equation of the type:

$$a^n + a_1 a^{n-1} + \ldots + a_n = 0$$

where all $a_i \in \mathcal{O}$.

The totality of elements of , integral over $\mathcal{O}$, is called the <u>integral closure</u> of $\mathcal{O}$ in K. If, for example, $\mathcal{O}$ = the ring of integers, and F = the field of complex numbers, then an element a satisfying an equation of the above type is called an algebraic integer.

Now, let S denote the set of all places of K which are finite on $\mathcal{O}$ (i.e., all places of K whose valuation rings contain $\mathcal{O}$).

We prove, first, that:

Theorem 3.1: If $a \in K$ is integral over $\mathcal{O}$, and if $\phi \in$ S, then ϕ is finite on a.

Proof: If $\phi(a) = \infty$, then $\phi(\frac{1}{a}) = 0$. Since a satisfies

$$(3.1) \qquad a^n + a_1 a^{n-1} + \ldots + a_n = 0$$

where all $a_i \in \mathcal{O}$, dividing by a^n, we get

$$(3.2) \qquad 1 + a_1 \frac{1}{a} + \ldots + a_n \frac{1}{a^n} = 0.$$

Applying $\phi \in$ S to (3.2), we have

$$1 = \phi(1) = 0$$

which is a contradiction.

Thus any place of K which is finite on $\mathscr{O}$ is finite on any element of K integral over $\mathscr{O}$.

From Theorem 3.1, we obtain the following:

Corollary 3.1: If F is a subfield of K, and if h is algebraic over F, and if ϕ is a place of K which is an isomorphism on F (i.e., a trivial place on F since the valuation ring of $\phi|F$ is F), then ϕ is an isomorphism on K (i.e., a trivial place of K).

Proof: We can, of course, view F as a subring of K, and, since K is algebraic over F, all elements of K are integral over F, so ϕ is finite on all elements of K which establishes the corollary.

We can also state the corollary in a slightly different manner. If ϕ is an isomorphism of F, then by the extension theorem we can extend ϕ to a place of K which, by the corollary, is a trivial place. Thus we can say: any place trivial on F has only trivial extensions to K.

Now, we wish to prove the converse of Theorem 3.1. Actually, we will prove more. Let $S_o \subset S$ consist of those places $\phi \in S$ whose kernel in $\mathscr{O}$ is a maximal ideal of $\mathscr{O}$.

Theorem 3.2: Let $a \in K$, and suppose $\phi(a) \neq \infty$ for any $\phi \in S_o$; then a is integral over $\mathscr{O}$ (and consequently $\phi(a) \neq \infty$ for any $\phi \in S$ by Theorem 3.1).

Proof: If $a = 0$, then $a \in \mathscr{O}$ and satisfies the equation $x = 0$, so we are done in this case. Thus we may assume that

60.

a $\neq$ 0. Consider the ring $\mathcal{O}_1 = \mathcal{O}[\frac{1}{a}]$. The theorem will be proved if we show that $\frac{1}{a}$ is a unit of $\mathcal{O}_1$, for this would mean that $a \in \mathcal{O}_1 = \mathcal{O}[\frac{1}{a}]$ whence

$$a = a_o + a_1\frac{1}{a} + \dots + a_r\frac{1}{a^r}$$

where all $a_i \in \mathcal{O}$. Multiplying by a^r, we get

$$a^{r+1} - a_o a^r - \dots - a_r = 0,$$

so a is integral over $\mathcal{O}$. Hence, we must just show that $\frac{1}{a}$ is a unit of $\mathcal{O}_1$. Suppose $\frac{1}{a}$ is not a unit of $\mathcal{O}_1$; then the ideal $\frac{1}{a}\mathcal{O}_1$ is not $\mathcal{O}_1$. But we know that we can find a maximal ideal $\mathcal{P}$ of $\mathcal{O}_1$ such that $\frac{1}{a}\mathcal{O}_1 \subset \mathcal{P}$. Now consider the map:

$$\mathcal{O}_1 \longrightarrow \mathcal{O}_1/\mathcal{P} .$$

$\mathcal{O}_1/\mathcal{P}$ is a field which we inject into $\overline{\mathcal{O}_1/\mathcal{P}}$, its algebraic closure. Thus we have a homomorphic map of the ring $\mathcal{O}_1$ into an algebraically closed field, and the homomorphism is non-trivial since $\mathcal{P} \neq \mathcal{O}_1$. Extend this homomorphism to a place ϕ of K. Since ϕ is finite on $\mathcal{O}_1$, ϕ is finite on $\mathcal{O}$. But $\frac{1}{a} \in \mathcal{P}$, so $\phi(\frac{1}{a}) = 0$, and, consequently, $\phi(a) = \infty$ which gives a contradiction if we use the set S in place of S_o in the statement of Theorem 3.2. We must finally show that the set S_o suffices. The kernel of ϕ in $\mathcal{O}_1$ is $\mathcal{P}$ which is a maximal ideal. The kernel

of ϕ in $\mathcal{U}$ is $\mathcal{U} \cap \mathcal{P} = \mathcal{M}$; we must show that $\mathcal{M}$ is a maximal ideal. We will show that if $a \in \mathcal{U}$, and $a \notin \mathcal{M}$, then a has an inverse mod $\mathcal{M}$, i.e., $\mathcal{U}/\mathcal{M}$ is a field, and, therefore, $\mathcal{M}$ is a maximal ideal. Thus if $a \in \mathcal{U}$, and $a \notin \mathcal{M}$, then $a \in \mathcal{U}_1$, and $a \notin \mathcal{P}$. Since $\mathcal{P}$ is a maximal ideal of $\mathcal{U}_1$, we know that a has an inverse in $\mathcal{U}_1$ mod $\mathcal{P}$, i.e.,

$$(3.3) \qquad a(b_0 + b_1 \frac{1}{a} + \ldots + b_r \frac{1}{a^r}) \equiv 1 \mod \mathcal{P} .$$

But $\frac{1}{a} \equiv 0 \mod \mathcal{P}$, so (3.3) reduces to

$$ab_0 \equiv 1 \mod \mathcal{P} ,$$

i.e., $ab_0 - 1 \in \mathcal{P}$, and, of course, $ab_0 - 1 \in \mathcal{U}$, so $ab_0 - 1 \in \mathcal{M}$. Hence $ab_0 \equiv 1 \mod \mathcal{M}$ which establishes the contention and finishes the proof of the theorem.

From Theorems 3.1 and 3.2, we know that the integral closure of $\mathcal{U}$ in K consists of all those elements of L which are finite on all places of S. From this, we obtain immediately that the integral closure, $\mathcal{O}$, of $\mathcal{U}$ in K forms a ring.

Now, let us show that the terminology integral closure is justified, i.e., we wish to show that the integral closure of $\mathcal{O}$ in K is $\mathcal{O}$ itself. Let S' denote the set of all places of K which are finite on $\mathcal{O}$. If $\phi \in S'$, then ϕ is finite on $\mathcal{O}$, and, therefore, finite

on $\mathcal{V}$, so $\phi \in S$. Conversely, if $\phi \in S$, then ϕ is finite on $\mathcal{O}$ since $\mathcal{O}$ is the integral closure of $\mathcal{V}$ in K, so $\phi \in S'$. Thus $S = S'$, and to see if any element a belongs to the integral closure of $\mathcal{O}$ in F, we must just test it on S. Hence the integral closure of $\mathcal{O}$ in K is precisely $\mathcal{O}$.

Finally, we observe that the integral closure $\mathcal{O}$ of $\mathcal{V}$ in K can be written as follows: $\mathcal{O} = \bigcap \overline{\mathcal{V}}$ where the intersection is taken over all valuation rings $\overline{\mathcal{V}}$ of K such that $\overline{\mathcal{V}} \supset \mathcal{V}$.

Chapter III

Absolutely Irreducible Varieties

§1. Introduction: Let V be an algebraic set over k, i.e.,
V consists of the zeros in Ω^n of an ideal $\mathscr{M}$ of k[X].
Now suppose we replace k by a larger field F, still con-
tained in Ω, and such that, over F, Ω has the usual
properties, i.e., Ω is an universal domain for F. Then
one can view V as an algebraic set over F. For we take
the ideal generated by $\mathscr{M}$ in F[X], i.e., $F\mathscr{M}$. This ideal
has the same zeros as $\mathscr{M}$, because $\mathscr{M} \subset F\mathscr{M}$, so if an ele-
ment of Ω^n annihilates $F\mathscr{M}$, then it surely annihilates
$\mathscr{M}$, and, conversely, if an element annihilates $\mathscr{M}$, then,
by the definition of $F\mathscr{M}$, it annihilates it. Thus V is
an algebraic set associated with the ideal $F\mathscr{M} \subset F[X]$, or,
in other words, V is also an algebraic set over F.

Now suppose that V is a variety over k. If we
extend k to F as before, it is not necessarily true that
V remains a variety over F. To see this, we consider the
following example. Let k = Q, the field of rational
numbers, and let $V = \left\{ \sqrt{2}, -\sqrt{2} \right\}$, i.e., the zero dimensional
variety consisting of the two points $\sqrt{2}$ and $-\sqrt{2}$. V
consists of the zeros of the ideal $(X^2 - 2)$. Let $F = Q(\sqrt{2})$,
or, for that matter, any field containing $\sqrt{2}$. Then V,
over F, splits into two varieties $\left\{ \sqrt{2} \right\} \cup \left\{ -\sqrt{2} \right\}$; since
now $\left\{ \sqrt{2} \right\}$ is a variety consisting of the zeros of the

ideal $(X - \sqrt{2})$, and similarly $\left\{-\sqrt{2}\right\}$ is a variety consist-
ing of the zeros of the ideal $(X + \sqrt{2})$.

Definition 1.1: A variety V over k is called absolutely
irreducible if it remains a variety over any extension
field F of k.

In this chapter, we intend to consider absolutely
irreducible varieties and determine conditions under which
a variety is absolutely irreducible. Before proceeding
to this discussion, we want first to consider the follow-
ing problem: we notice in the example just given that the
variety over the extended field split into two varieties
of the same dimension; we want to show that this is true
in general. We have also seen in Chapter I that the
product of two varieties is not necessarily a variety.
Again, we want to show that the product splits into com-
ponents each of the same dimension.

§2. Algebraically free fields: In order to prove the
above stated conjectures, we must introduce a new concept.

Definition 2.1: Let E and F be two fields over k. If (y)
is a transcendence base of F over k, and if (y) is alge-
braically independent over E, then we say that F is alge-
braically free over E.

It can readily be seen that this is a symmetric
property, and we say simply, for two such fields E and F,
that E and F are algebraically free over k.

All fields that we will talk about are meant to lie in Ω. We denote by EF the smallest field containing both L and F, and we will denote the algebraic closure of a given field by placing a bar over it. We want to prove now the following important lemma.

Lemma 2.1: Let ϕ be given place of $E \to \Omega \cup \infty$ such that $\phi|_k = 1_k$ (i.e., the restriction of ϕ to k).
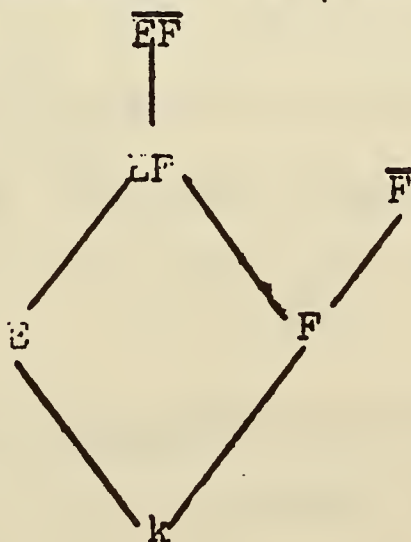
Moreover, let L and F be algebraically free over k. Then there exists a place $\tilde{\phi}$ of $\overline{EF}$ where $\tilde{\phi}|_F = 1_F$, and where $\tilde{\phi}$ acts on σE, where σE is a field isomorphic to E, as ϕ does on E.

Proof: Let $\mathcal{M}$ be the valuation ring of ϕ, and let (y) be a given transcendence base of F over k. Extend ϕ to $\mathcal{M}[y] \to \Omega$ by letting this map act on $\mathcal{M}$ as ϕ does and letting it take (y) $\to$ (y) (i.e., each component is left fixed). Since F is algebraically free over L, this map is well-defined and, consequently, a homomorphism. Now, by the Extension Theorem, we can extend this homomorphism to a place ϕ_o of $\overline{EF}$:

$$\phi_o : \overline{EF} \longrightarrow \Omega \cup \infty,$$

and clearly

$$\phi_o \Big|_{k(y)} = 1.$$

In particular, ϕ_o is trivial on $k(y)$. But F is algebraic over $k(y)$ and $\overline{F}$ is algebraic over F, so $\overline{F}$ is algebraic over $k(y)$. Applying Corollary 3.1 of Chapter II, we know that ϕ_o is trivial on F, i.e., an isomorphism on $\overline{F}$. This isomorphism maps $\overline{F}$ into the algebraic closure of the image of $k(y)$: consequently, into $\overline{F}$. Thus

$$\phi_o \Big|_{\overline{F}} = \tau$$

where τ is an automorphism of $\overline{F}\big|_{k(y)}$ (i.e., an automorphism of $\overline{F}$ which leaves $k(y)$ fixed).

Now extend this automorphism τ to an automorphism σ of $\overline{EF}$ in the following manner: select a transcendence base (x) of $\overline{F}$ over k and extend τ to $\overline{F}(x)$ by letting $(x) \longrightarrow (x)$. This extended map is obviously an automorphism since (x) is independent over $\overline{F}$. Now $\overline{EF}$ is algebraic over $\overline{F}(x)$ and we have an automorphism of $\overline{F}(x)$, we can extend this automorphism to an isomorphism of $\overline{F}(x)(a)$ where $a \in \overline{EF}$ by the usual procedure of modern algebra.[*] We order all these extensions as was done in the Extension Theorem. Applying Zorn's lemma to the inductively ordered set, we obtain a maximal element which it is easy

---

[*] See, for example, Van der Waerden, Modern Algebra, Volume 1, p. 108, Ungar Publishing Co.

to see must be an automorphism of $\overline{EF}$, for otherwise we could extend this maximal element to a larger field. The interested reader should really supply the full details to this argument.

Hence, we have extended τ to an automorphism σ of $\overline{EF}$, and, of course,

$$\tau = \phi_o|_{\overline{F}} = \sigma|_{\overline{F}} \ .$$

Now, we define $\widetilde{\phi} = \phi_o\sigma^{-1}$, which is clearly a place of $\overline{EF}$. Also, $\widetilde{\phi}|_{\overline{F}} = 1_{\overline{F}}$, so $\widetilde{\phi}|_F = 1_F$. Finally $\widetilde{\phi}|_{\sigma E} = \phi\sigma^{-1}$, so $\widetilde{\phi}$ acts on σE as ϕ does on E, and the lemma has been established in full.

We can now answer the first conjecture posed at the end of section 1 of this chapter. Namely,

Theorem 2.1: Let V be a variety over k and let F be an extension field of k such that Ω is an universal domain for F. If, over F, V splits into component varieties, then all these varieties have the same dimension.

Proof: Let (x) be generic point of V over k, and such that (x) is algebraically free over F, i.e., the transcendental part of (x) over k is algebraically independent over F. Such a choice is possible since Ω is an universal domain for F. Let $L = k(x)$, and let $(\xi) \in V$; then $(x) \xrightarrow{k} (\xi)$, i.e., $k[x] \longrightarrow k[\xi]$ is a homomorphism. We know, by the example in section 1, that we cannot conclude that $(x) \xrightarrow{F} (\xi)$ since, as we saw, $-\sqrt{2}$ is a specialization of

$\sqrt{2}$ over Q but not over $Q(\sqrt{2})$. However, let us extend the homomorphism $k[x] \longrightarrow k[\xi]$ to a place ϕ of L. Then by lemma 2.1, we can find an automorphism σ such that $\check{\phi} = \phi_0 \sigma^{-1}$ is identity on F and acts on $\sigma E = k(\sigma x)$ as ϕ does on E, namely, $(\sigma x) \xrightarrow{F} (\xi)$, and, by the proof of lemma 2.1, we can insist that σ leaves a transcendence base of (x) fixed. But (x) and (σx) are equivalent generic points of V over k since σ is an automorphism which is identity on k; of course, (x) and (σx) are not necessarily equivalent over F since σ does not necessarily leave F fixed. Therefore, (σx) is now possibly the generic point of another variety, and (ξ) lies over F in the component variety whose generic point is (σx). Now

$$\dim_F (x) = \dim_k (x) = \dim_k (\sigma x) = \dim_F (\sigma x).$$

The first equality follows from the fact that (x) is algebraically free over F; the second from the fact that (x) and (σx) are equivalent generic points over k; and the third from the fact that σ keeps the transcendence base fixed. Hence, we see that all components of V over F have the same dimension as that of V over k, and the proof is completed.

Furthermore, we can now say that the number of components that a variety splits into over an extension

field is bounded since the number of possible σ's is bounded, for σ leaves the transcendence base of (x) fixed, and, thus, can only act non-identically on the algebraic part of (x), and, therefore from basic theorems in modern algebra on the extensions of an isomorphism[*], we know that the number of σ's is bounded.

Finally, let us prove the second conjecture of section 1.

<u>Theorem 2.2</u>: Let V be a variety over k and W a variety over k. Then if V$\times$W over k splits into component varieties, all of them are of the same dimension, namely, dimV + dimW.

<u>Proof</u>: Let (x) be a generic point of V over k, and let (y) be a generic point of W over k, and select (x) and (y) so that they are algebraically free which is, of course, possible by the nature of Ω. Suppose $(x) \xrightarrow{k} (\xi)$ and $(y) \xrightarrow{k} (\eta)$, i.e., $(\xi,\eta) \in V \times W$. We know that it is false that $(x,y) \xrightarrow{k} (\xi,\eta)$ since the product of two varieties is not necessarily a variety. Let us see what we can achieve. Clearly, we can't achieve $(\xi,y) \xrightarrow{k(\xi)} (\xi,\eta)$, for this would mean $(y)\xrightarrow{k(\xi)} (\eta)$; however, from the proof of Theorem 2.1, we know that we

---

[*]   See van der Waerden, Modern Algebra, Vol. I, p. 108 and pp. 121-122.

achieve

$$(\sigma y) \xrightarrow{k(\xi)} (\eta)$$

where σ is an automorphism, and where we must choose
(y) algebraically free from (ξ).

Similarly, we know that we can't achieve
$(x, \sigma y) \xrightarrow{k(\sigma y)} (\xi, \sigma y)$ since this is the same as
$(x) \xrightarrow{k(\sigma y)} (\xi)$, but we can achieve

$$(\sigma' x) \xrightarrow{k(\sigma y)} (\xi)$$

where σ' is an automorphism, and where (x) and (y)
must be algebraically free.

Thus, we have

$$(\sigma' x, \sigma y) \xrightarrow{k} (\xi, \sigma y) \xrightarrow{k} (\xi, \eta),$$

so

$$(\sigma' x, \sigma y) \longrightarrow (\xi, \eta),$$

and we can conclude as in Theorem 2.1 that each com-
ponent of the product variety is of the same dimension,
namely, dimV + dimW.

§3. Linear Disjointness: In this and the following
sections of this chapter, we want to analyze absolutely
irreducible varieties. First, we want to obtain criteria
for a variety to be absolutely irreducible. To this
end, we introduce the concept of linear disjointness

of two fields which is much stronger than being alge-
braically free.

All fields are again meant to lie in Ω. We define:

Definition 3.1: Two fields E and F are called linearly
disjoint over k if elements $a_1,\ldots,a_m \in F$ are linearly
independent over E whenever they are linearly independent
over k.

First, we wish to show that this is a symmetric
property. Thus let E and F be linearly disjoint, and
suppose $\beta_1,\ldots,\beta_m \in E$ are linearly independent over k.
We wish to show that they are linearly independent over F.
Suppose this is false; then

$$a_1 \beta_1 + \ldots + a_m \beta_m = 0$$

with all $a_\nu \in F$ and non-trivially (i.e., not all $a_\nu = 0$).
Let $\omega_1,\ldots,\omega_r \in F$ be linearly independent over k, and
such that

$$a_1,\ldots,a_m \in k\omega_1 + \ldots + k\omega_r.$$

Then

$$a_i = \sum_{\nu=1}^{r} a_{i\nu}\omega_\nu$$

where all $a_{i\nu} \in k$. Since $\sum_{i=1}^{m} a_i \beta_i = 0$, we get

$$\sum_{\nu=1}^{r} \left(\sum_{i=1}^{m} a_{i\nu}\beta_i\right)\omega_\nu = 0$$

where $\displaystyle\sum_{i=1}^{m} a_{1\nu}\beta_1 \in E$ for all ν. Since the ω's are inde-

pendent over k and since E and F are linearly disjoint,

we get

$$\sum_{i=1}^{m} a_{1\nu}\beta_1 = 0$$

for all ν. But the β's are linearly independent over k.

Consequently, $a_{1\nu} = 0$ for all i and ν, which implies that

all $_1 = 0$ which is a contradiction, and the proof is

completed.

It is immediately apparent that if two fields

are linearly disjoint, then any two subfields of them

are linearly disjoint.

Now, we want to see if there is an easy criterion

for two fields to be linearly disjoint. We first show:

Theorem 3.1: If F and $\overline{K}$ are linearly disjoint over k,

and E and F are algebraically free over k, then E and F

are linearly disjoint over k.
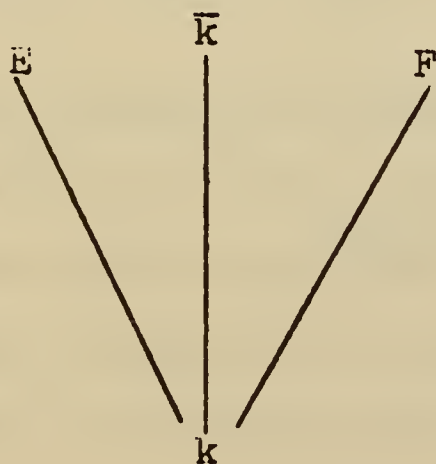
Proof:

Construct a place $\phi: E \longrightarrow \overline{K} \cup \infty$
which is identity on k. This
can clearly be done by applying
the Extension Theorem to the
homomorphism $k \xrightarrow{j} \overline{K}$ where i
is the injection map. Since
E and F are algebraically free,

we can construct ϕ_o and σ according to the proof of lemma 2.1 such that $\phi_o\big|_E = \phi$ and $\phi_o\big|_F = \sigma$.

Suppose that

$$(3.1) \qquad \beta_1 a_1 + \ldots + \beta_m a_m = 0$$

where all $\beta_i \in E$, and not all $\beta_i = 0$, and where all $a_j \in F$ and are linearly independent over k. Let $|\;|$ be the valuation belonging to the place ϕ_o. Let, say,

$$|\beta_1| = \text{Max}_\nu \; (|\beta_\nu|) \neq 0.$$

From (3.1), we get

$$(3.2) \qquad a_1 + \frac{\beta_2}{\beta_1} a_2 + \ldots + \frac{\beta_m}{\beta_1} a_m = 0$$

where, for all i, $\left|\frac{\beta_i}{\beta_1}\right| \leq 1$ but this implies that $\frac{\beta_i}{\beta_1} \in \mathcal{O}$, the associated valuation ring. Hence $\phi_o(\frac{\beta_i}{\beta_1}) \neq \infty$ for all i. Applying ϕ_o to (3.2), we get

$$(3.3) \qquad \sigma(a_1) + \lambda_2 \sigma(a_2) + \ldots + \lambda_m \sigma(a_m) = 0$$

where all $\lambda_i \in \overline{k}$. Finally, applying σ^{-1} to (3.3) we have

$$(3.4) \qquad 1 \cdot a_1 + \sigma^{-1}(\lambda_2)a_2 + \ldots + \sigma^{-1}(\lambda_m)a_m = 0.$$

But $\sigma^{-1}: \overline{k} \to \overline{k}$, so all the coefficients of (3.4) belong to $\overline{k}$, and not all are 0, but this contradicts the fact that F and $\overline{k}$ were assumed linearly disjoint over k.

Next, let us see if there is a good criterion for
$\overline{k}$ and F to be linearly disjoint. If k is algebraically
closed in F (i.e., F contains no elements algebraic over
k other than k itself), and k is of characteristic 0,
then we can show that F and $\overline{k}$ are linearly disjoint.
If k is not of characteristic 0, then we must add another
condition, namely:

<u>Theorem 3.2</u>: If k, of characteristic p, is algebraically
closed in F, and if F and $k^{1/p}$ are linearly disjoint, then
F and $\overline{k}$ are linearly disjoint.

<u>Proof</u>: We first observe that whenever $a_1, \ldots, a_n \in F$
are linearly independent over k, then $a_1^p, \ldots, a_n^p$ are also
linearly independent over k. For if

$$c_1 a_1^p + \ldots + c_n a_n^p = 0$$

with all $c_i \in k$ and not all $c_i = 0$, then

$$c_1^{1/p} a_1 + \ldots + c_n^{1/p} a_n = 0$$

where all $c_i^{1/p} \in k^{1/p}$ and not all $c_i^{1/p} = 0$, but this
contradicts the fact that $k^{1/p}$ and F are linearly disjoint.

Now suppose $\beta_1, \ldots, \beta_n \in \overline{k}$, and suppose $a_1, \ldots, a_n \in F$
are linearly independent over k and such that

$$\beta_1 a_1 + \ldots + \beta_n a_n = 0$$

with not all $\beta_i = 0$. Then we have

$$\beta_1^{p^s} \alpha_1^{p^s} + \ldots + \beta_n^{p^s} \alpha_n^{p^s} = 0$$

where $\alpha_1^{p^s}, \ldots, \alpha_n^{p^s}$ are still linearly independent over k
by the previous argument. By taking s big enough we can
assume that all $\beta_i^{p^s}$ are separable with respect to k.
Thus, changing notation, we can assume that $\beta_1, \ldots, \beta_n$
are separable, and now the proof proceeds as in the case
of characteristic 0. Namely, the field $k(\beta_1, \ldots, \beta_n)$ can
be generated by one element γ, i.e., $k(\beta_1, \ldots, \beta_n) = k(\gamma)$.
Thus we have

(3.5) $$g_1(\gamma)\alpha_1 + \ldots g_n(\gamma)\alpha_n = 0$$

where the g_i are polynomials in γ, and where, for all i,
$\deg. g_i(x) < \deg. \gamma$. Of course, (3.5) can be viewed as an
equation γ satisfies over F, and it is not possible for
all coefficients to be zero since the α's are linearly
independent over k; thus we get

(3.6) $$\deg._F \gamma < \deg._k \gamma$$

where $\deg._F$ indicates the degree over F. Now we will
show that (3.6) yields a contradiction. Let $P = Irr.(\gamma, k)$

(i.e., the irreducible equation satisfied by γ over k),
and let $Q = Irr.(\gamma, F)$. Then $Q(x)|P(x)$ properly by (3.6).
But this implies that all roots of $Q(x)$ are algebraic
over k, and, consequently, the coefficients of $Q(x)$ are
algebraic over k since they are formed by algebraic
combinations of the roots. Hence the coefficients of
$Q(x)$, which belong to F are algebraic over k and, there-
fore, belong to k. This plus the fact that $Q(x)|P(x)$
properly implies that $P(x)$ is not irreducible which is
a contradiction, and the theorem has finally been
established.

We will now apply these results to the question
of when a variety is absolutely irreducible.

Let V be a variety over k with the generic point
(x), and the prime ideal $\mathscr{Y}x|_k$, i.e.,

$$\mathscr{Y}x|_k = \left\{ f(X)\,|\,f(X) \in k[X] \text{ and } f(x) = 0 \right\}.$$

We want to see what $\mathscr{Y}x|_F = \left\{ f(X)\,|\,f(X) \in F[X] \text{ and } f(x) = 0 \right\}$
is. That is, we want to see what the connection between
$\mathscr{Y}x|_k$ and $\mathscr{Y}x|_F$ is, under the assumption that F and k(x)
are linearly disjoint over k.

Suppose $f(X) \in \mathscr{Y}x|_F$, so $f(X) \in F[X]$, and $f(x) = 0$.

Let $a_1, \ldots, a_m$ be the maximal number of coefficients of $f(X)$ which are linearly independent over k. Then all coefficients of $f(X)$ are linear combinations of the a_i with coefficients in k. This leads to a formula:

$$f(X) = a_1 \phi_1(X) + \ldots + a_m \phi_m(X)$$

where all $\phi_i(X) \in k[X]$. Now

$$0 = f(x) = a_1 \phi_1(x) + \ldots + a_m \phi_m(x),$$

but F and $k(x)$ are linearly disjoint; whence, each $\phi_i(x) = 0$, i.e., $\phi_i(X) \in \mathscr{Y}_{x}|_k$. Thus $f(X) \in \mathscr{Y}_{x}|_k{}^F$, and we have $\mathscr{Y}_x|_F \subset \mathscr{Y}_x|_k{}^F$. Trivially, we have $\mathscr{Y}_x|_k{}^F \subset \mathscr{Y}_x|_F$. Hence

(3.7) $\quad \mathscr{Y}_x|_F = \mathscr{Y}_x|_k{}^F.$

Especially, $\mathscr{Y}_x|_F$ and $\mathscr{Y}_x|_k$ have the same zeros; hence, V is also a variety over F. Also, (3.7) is equivalent to the fact that $\mathscr{Y}_x|_F$ has a basis consisting of polynomials in $k[X]$. The implication one way is trivial since if $\mathscr{Y}_x|_F = \mathscr{Y}_x|_k{}^F$, then it suffices to have a basis for $\mathscr{Y}_x|_k$ and F.

78.

For the converse, we consider in general an ideal $\mathcal{O}\mathcal{l} \subset F[X]$. Let $\mathcal{O}\mathcal{l}_o = \mathcal{O}\mathcal{l} \cap k[X]$, so $\mathcal{O}\mathcal{l}_o \subset \mathcal{O}\mathcal{l}$. Suppose $\mathcal{O}\mathcal{l}$ has a basis in $k[X]$. Let $\psi_1(X), \ldots, \psi_r(X)$ be a basis of $\mathcal{O}\mathcal{l}_o$; then $\psi_1(X), \ldots, \psi_r(X)$ is also a basis for $\mathcal{O}\mathcal{l}$, and $\mathcal{O}\mathcal{l} = \mathcal{O}\mathcal{l}_o F$.

Now, employing the same notation, we have:

Lemma 3.1: Suppose $\mathcal{O}\mathcal{l} = \mathcal{O}\mathcal{l}_o F$. Let $\phi(X) \in \mathcal{O}\mathcal{l}$, and suppose that

$$\phi(X) = \sum_{i=1}^{m} a_i P_i(X)$$

where the a_i are linearly independent over k, and where the $P_i(X) \in k[X]$ (we have seen previously that such a form can be achieved). Then each $P_i(X) \in \mathcal{O}\mathcal{l}$, and hence to $\mathcal{O}\mathcal{l}_o$.

Proof: We can write

$$(3.8) \qquad \phi(X) = \sum_{j=1}^{n} \beta_j Q_j(X)$$

where the $Q_j(X) \in \mathcal{O}\mathcal{l}_o$, and the $\beta_j \in F$ since $\mathcal{O}\mathcal{l} = \mathcal{O}\mathcal{l}_o F$. We assume that n is minimal, i.e., of all such ways of expressing $\phi(X)$, (3.8) is the shortest. Then the β_j are linearly independent over k, for if not, we could express $\phi(X)$ in a shorter form. Now, let us study

(3.9) $$\sum_{i=1}^{m} \alpha_i P_i(X) = \sum_{j=1}^{n} \beta_j Q_j(X).$$

Comparing coefficients, we get a system of linear equations with coefficients in k, namely,

(3.10) $$L(\beta_j) = M(\alpha_i).$$

Of course, the system (3.10) has one solution, but we claim that it can't have more than one solution, i.e., for given α_i, we claim the system has at most one solution, for otherwise the system

$$L(\beta_j) = 0$$

would have a non-trivial solution. This non-trivial solution would come from the case where all $\alpha_i = 0$, i.e., from the case

$$\sum_{j} \beta_j Q_j(X) = 0 ,$$

but this would imply that the β_j are dependent over k which is a contradiction. Thus the system (3.10) has only one solution, so

$$\beta_j = \sum_{i=1}^{m} a_{ji}\alpha_i$$

where all $a_{ji} \in k$. Substituting this in (3.9), we have

$$\sum_{i=1}^{m} a_i P_i(X) = \sum_{i=1}^{m} a_i \sum_{j=1}^{n} a_{ji} Q_j(X)$$

where $\sum_{j=1}^{n} a_{ji} Q_j(X) \in k[X]$. But the a_i are independent over k; whence

$$P_i(X) = \sum_{j=1}^{n} a_{ji} Q_j(X) \in \mathcal{U}.$$

for each i which finishes the proof.

We saw previously that if F and k(x) are linearly disjoint over k that then $\mathcal{Y}_x|_F = \mathcal{Y}_x|_k F$. We are now in a position to prove the converse of this, namely:

__Theorem 3.3__: If $\mathcal{Y}_x|_F = \mathcal{Y}_x|_k F$, then k(x) and F are linearly disjoint over k.

__Proof__: If k(x) and F were not linearly disjoint over k, then we could find elements $a_1, \ldots, a_n \in F$ which are independent over k but not independent over k(x), i.e.,

(3.11) $\qquad a_1 \phi_1(x) + \ldots + a_n \phi_n(x) = 0$

where all $\phi_i(x) \in k(x)$ and not all $\phi_i(x) = 0$. Clearing the denominations in (3.11), we may assume that all $\phi_i(x) \in k[x]$. Then

$$a_1 \phi_1(X) + \ldots + a_n \phi_n(X) \in \mathcal{Y}_x|_F.$$

and, applying lemma 3.1, we get that each $\phi_1(X) \in \mathcal{Y}_x|_k$

which means that each $\phi_1(x) = 0$ which is a contradiction.

Now let us apply the concept of linear disjointness to the question of when the product of two varieties is a variety. Suppose that $k(x)$ and $k(y)$ are linearly disjoint. We want to see how we can then express $\mathcal{Y}_{(x,y)}|_k$.

Let $f(X,Y) \in \mathcal{Y}_{(x,y)}|_k$, so $f(x,y) = 0$, and the coefficients of $f(X,Y)$ belong to k. Consider $f(X,y)$. Let $\phi_1(y),\dots\phi_m(y) \in k[y]$ be the maximal number of coefficients of $f(X,y)$ linearly independent over k. Then

$$f(X,y) = \phi_1(y)\,\phi_1(X) + \dots + \phi_m(y)\,\phi_m(X)$$

where each $\phi_1(X) \in k[X]$. But

$$0 = f(x,y) = \phi_1(y)\,\phi_1(x) + \dots + \phi_m(y)\,\phi_m(x),$$

and since $\phi_1(y),\dots,\phi_m(y)$ are linearly independent over k, we get by the linear disjointess of $k(x)$ and $k(y)$ that each $\phi_1(x) = 0$, so each

$$\phi_1(X) \in \mathcal{Y}_x|_k.$$

Now put

$$g(X,Y) = f(X,Y) - (\phi_1(Y)\phi_1(X) + \dots + \phi_m(Y)\phi_m(X)).$$

Then $g(X,y) = 0$. Write

$$g(X,Y) = \sum_{\mu(X)} \mu(X)\psi_\mu(Y)$$

where $\mu(X)$ ranges over the monomials of X (i.e.,
$\mu(X) = X_1^{\nu_1} X_2^{\nu_2} \ldots X_n^{\nu_n}$). Then

$$\sum_{\mu(X)} \mu(X)\psi_\mu(y) = 0$$

which implies that $\psi_\mu(y) = 0$, so $\psi_\mu(Y) \in \mathscr{Y}_{y}|_k$. Thus

$$g(X,Y) \in k[X]\mathscr{Y}_{y}|_k,$$

and, consequently,

$$f(X,Y) \in k[X]\mathscr{Y}_{y}|_k + k[Y]\mathscr{Y}_{x}|_k.$$

Hence,

$$\mathscr{Y}_{(x,y)}|_k \subset k[X]\mathscr{Y}_{y}|_k + k[Y]\mathscr{Y}_{x}|_k.$$

The reverse inclusion is trivial, for clearly any poly-
nomial of $k[X]\mathscr{Y}_{y}|_k + k[Y]\mathscr{Y}_{x}|_k$ vanishes for $(X) = (x)$,
and $(Y) = (y)$. Therefore, we have obtained

$$(3.12) \quad \mathscr{Y}_{(x,y)}|_k = k[X]\mathscr{Y}_{y}|_k + k[Y]\mathscr{Y}_{x}|_k.$$

Finally, let (x) be a generic point of V, which consists of the zeros of $\mathcal{Y}_x|_k$, and let (y) be a generic point of W, which consists of the zeros of $\mathcal{Y}_y|_k$. If k(x) and k(y) are linearly disjoint, then we claim that (x,y) is a generic point of V⨯W. For, since k(x) and k(y) are linearly disjoint, (3.12) is valid. Thus

$$\mathcal{Y}_x|_k \subset \mathcal{Y}_{(x,y)}|_k$$

and

$$\mathcal{Y}_y|_k \subset \mathcal{Y}_{(x,y)}|_k$$

so a zero of $\mathcal{Y}_{(x,y)}|_k$ must make all of $\mathcal{Y}_x|_k$ vanish and also all of $\mathcal{Y}_y|_k$ vanish so it must be of the form (ξ,η) where $(\xi)\in V$, and $(\eta)\in W$, and, conversely, any element of V⨯W is a zero for $\mathcal{Y}_{(x,y)}|_k$. Thus

$$\{(x,y)\} \longrightarrow \mathcal{Y}_{(x,y)}|_k \longrightarrow V\times W,$$

so if k(x) and k(y) are linearly disjoint where (x) is a generic point of V, and where (y) is a generic point of W, then V⨯W remains a variety.

Now let us collect some of these results. Let V be a variety over k, and let F be an extension field of

k (with Ω still a universal domain for it). We ask:
Is V a variety over F? We select a generic point (x)
in such a way that F and k(x) are algebraically free
which is, of course, possible by the nature of Ω. Now
we must assume that:

    1) k is algebraically closed in k(x),

    2) $k^{1/p}$ and k(x) are linearly disjoint over k.

Then applying Theorems 3.2 and 3.1 we know that F and
k(x) are linearly disjoint over k, and, therefore, as
we've seen, V is a variety over F. Thus if the generic
point (x) satisfies conditions 1) and 2) (which are
independent of F since $k(x) \cong k(y)$ where y is another
generic point), then the variety is absolutely irreducible.
A variety having such a generic point is called a
<u>regular variety</u>, and the generic point is called a
<u>regular point</u>.

    If the ground field k is algebraically closed,
then conditions 1) and 2) are automatically satisfied
(since $k^{1/p} = k$ for k algebraically closed), so in this
case, all varieties are regular.

    Let us now consider the product of two varieties
$V \times W$. Let (x) be a generic point of V, and let (y) be a

generic point of W, and choose them so that $k(x)$ and $k(y)$ are algebraically free. If one of the factors, say, V is regular, then $k(x)$ is linearly disjoint from any field of which it is algebraically free, so $k(x)$ and $k(y)$ are linearly disjoint; then, as we've seen, $V \times W$ is a variety. Thus if one factor of the product is regular, then the product remains a variety.

Before proceeding to the next section, we want to investigate a little more thoroughly the concept of linear disjointness; the results obtained will be applied in the following section.

The first thing that we want to show is that linear disjointness is transitive, i.e.

Lemma 3.2: E and F are linearly disjoint over k if and

only if:
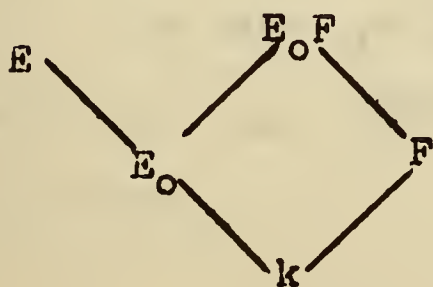
a) E_0 and F are linearly disjoint over k and

b) E and E_0F are linearly disjoint over E_0.

Proof: Suppose E, F are linearly disjoint over k. Then a) is, of course, satisfied. Let us show that b) is also satisfied. Let $a_1, \ldots, a_m \in E$ be linearly independent over E_o. Suppose

$$(3.13) \qquad a_1 A_1 + \ldots + a_m A_m = 0$$

non-trivially, and where all $A_i \in E_o F$. $E_o F$ consists of the totality of $\dfrac{\sum_\mu \beta_\mu \gamma_\mu}{\sum_\mu \beta'_\mu \gamma'_\mu}$ where the sums are finite, and where all β_μ, $\beta'_\mu \in E_o$ and γ_μ, $\gamma'_\mu \in F$. Clearing denominators in (3.13), we can assume that

$$A_1 = \sum_\nu \beta_{1\nu} \gamma_{1\nu}$$

where all $\beta_{1\nu} \in E_o$ and all $\gamma_{1\nu} \in F$. Let $\gamma_1, \ldots, \gamma_\nu \in F$ be the maximal number of linearly independent $\gamma_{1\nu}$ over k. Expressing each $\gamma_{1\nu}$ in terms of them, we get

$$A_1 = \sum_\nu \gamma_\nu \beta'_{1\nu}$$

where all $\beta'_{1\nu} \in E_o$. Now, since $\sum a_1 A_1 = 0$, we have

$$\sum_{1,\nu} a_1 \beta'_{1\nu} \gamma_\nu = 0.$$

But the γ_ν are independent over k, and $\sum_i a_i \beta'_{i\nu} \in E$; hence by the linear disjointness of E and F, we obtain

$$\sum_i a_i \beta'_{i\nu} = 0$$

for each ν. But the a_i were taken linearly independent over E_o. Consequently $\beta'_{i\nu} = 0$ for all i and ν, and this implies that each $A_i = 0$ which is a contradiction.

Conversely, let us assume that a) and b) are satisfied; we wish to show that then E, F are linearly disjoint over k. Let $a_1, \ldots, a_m \in F$ be linearly independent over k. Suppose $\sum_i e_i a_i = 0$ non-trivially with each $e_i \in E$. Let the maximal number of linearly independent e_i over E_o be $e_1^*, \ldots, e_s^*$. Then $e_i = \sum_\mu g_{i\mu} e_\mu^*$ where each $g_{i\mu} \in E_o$. Then we have

$$\sum_{i,\mu} a_i g_{i\mu} e_\mu^* = 0,$$

but, since the e_μ^* are independent over E_o, by condition b), we get

$$\sum a_i g_{i\mu} = 0$$

for each μ. Finally since the a_i are independent over k, we get by condition a) that $g_{i\mu} = 0$ for all i and μ

which implies that each $e_i = 0$, and this gives a contradiction.

Next, we want to show that to establish whether two fields are linearly disjoint it suffices to test a basis. Namely:

Lemma 3.3: E and F are linearly disjoint over k if and only if a basis of F over k remains linearly independent over E.

Proof: Let $\{\omega\}$ be a basis of F over k. If E and F are linearly disjoint, then, of course, $\{\omega\}$ is linear independent over E.

Suppose, conversely, that $\{\omega\}$ is linearly independent over E. Take $a_1,\ldots,a_n \in F$ and linearly independent over k. Then

$$a_i = \sum_\omega a_{i\omega}\,\omega$$

where each $a_{i\omega} \in k$ and where the sum is finite. Suppose

$$\sum_i b_i a_i = 0$$

with each $b_i \in E$. Then

$$\sum_\omega \sum_i b_i a_{i\omega}\omega = 0$$

which implies that

$$\sum_i b_1 a_{1\omega} = 0$$

for all ω in question since the ω are linearly independent over E. Thus we get a system of linear equations with coefficients $a_{1\omega} \in k$ and unknowns $b_1 \in E$. Hence, if the b_1 are non-trivial, we can also solve for them in k. Call these solutions $\overline{b_1}$. Then we have $\sum_i \overline{b}_1 a_1 = 0$ which contradicts the fact that the a_1 are linearly independent over k, and the lemma is established in full.

If the F of lemma 3.3 should be the quotient field of a ring $\mathcal{O}$ containing k, then it suffices to test a basis $\{\omega\}$ of $\mathcal{O}$. For suppose $a_1, \ldots, a_n \in F$ are linearly independent over k. Let $\{\omega\}$ be a basis of $\mathcal{O}$. $a_1 = \dfrac{a_1'}{a_1''}$ where $a_1', a_1'' \in \mathcal{O}$. Suppose

$$\sum_i b_1 a_1 = 0$$

where each $b_1 \in E$; then $\sum_i b_1 \dfrac{a_1'}{a_1''} = 0$, or $\sum_i b_1 \tilde{a}_1 = 0$

where each $\tilde{a}_1 \in \mathcal{O}$, so $\tilde{a}_1 = \sum a_{1\omega} \omega$ with $a_{1\omega} \in k$. Thus

$$\sum_\omega \sum_i b_1 a_{1\omega} \omega = 0,$$

and, arguing as before, we get $\bar{b}_1 \in k$ such that $\sum_1 \bar{b}_1 \tilde{a}_1' = 0$; hence $\sum_1 \bar{b}_1 a_1 = 0$ which is a contradiction.

§4. <u>Separably generated fields</u>: In analyzing sufficient conditions for a variety to be absolutely irreducible, one of the conditions we needed fulfilled was that $k^{1/p}$ and $k(x)$ are linearly disjoint over k. In this section, we want to see, in general, what F and $k^{1/p}$ being linearly disjoint over k means. The first theorem, in this respect, which we want to establish is the following:

<u>Theorem 4.1</u>: If F and $k^{1/p}$ are linearly disjoint over k, and if $F = k(a)$ where a is algebraic over k, then a is separable, and, conversely, if $F = k(a)$ where a is separable with respect to k, then F and $k^{1/p}$ are linearly disjoint over k.

<u>Proof</u>: Suppose $F = k(a)$, where a is algebraic over k. Let $P = Irr.(a,k)$, and let $n = deg.P$. Then $1, a, \ldots, a^{n-1}$ is a basis of F/k. If F and $k^{1/p}$ are not linearly disjoint, then this basis becomes algebraically dependent over $k^{1/p}$. Hence, over $k^{1/p}$, a satisfies an irreducible equation $Q = Irr.(a, k^{1/p})$ where $deg.Q < deg.P$. Now, $(Q(X))^p \in k[X]$ and has a as a root. Therefore, $P(X) | (Q(X))^p$. If $P(X)$

were separable, then $P(X) \mid Q(X)$ which is a contradiction since deg.$Q <$ deg.P. Thus we have shown that if F and $k^{1/p}$ are not linearly disjoint then a is not separable.

Now, suppose that a is not separable. Then $P(X)$ can be expressed as a polynomial in X^p, namely, $P(X) = \phi(X^p)$ where deg.$\phi = \frac{n}{p}$. But $\phi^{1/p}(a) = 0$ since $\phi(a^p) = 0$, so extracting the p-th root we clearly get the result. Thus $1, a, \ldots, a^{n/p}$ are linearly dependent over $k^{1/p}$, and, consequently, F and $k^{1/p}$ are not linearly disjoint, and the proof is completed.

Continuing in this manner, we now show:

Theorem 4.2: Suppose $F = k(x)$ is a purely transcendental extension (i.e., (x) is a transcendence base of F); then F and $k^{1/p}$ are linearly disjoint over k.

Proof: F is the quotient field of $\mathscr{S} = k[x] \supset k$. A basis of $\mathscr{S}/k$ is the monomials ν. If we had $\sum_\nu a_\nu \nu = 0$ with $a_\nu \in k^{1/p}$, then $\sum_\nu a_\nu^p \nu^p = 0$, but the ν^p range over distinct monomials. Thus each $a_\nu^p = 0$, so each $a_\nu = 0$, and using the comment following lemma 3.3 of the preceding section, we get that F and $k^{1/p}$ are linearly disjoint.

We observe at this point that $k^{1/p}$ and F are linearly

disjoint over k if and only if $k^{1/p}$ and every finitely generated subfield of F are linearly disjoint over k. For if $k^{1/p}$ and F are linearly disjoint, then, of course, any subfield of F and $k^{1/p}$ are linearly disjoint. Conversely, let $k^{1/p}$ and every finitely generated subfield of F be linearly disjoint. Let $a_1, \ldots, a_n \in F$ be linearly independent over k. Then

$$a_1 \in F_1 = k(\beta_1^{(1)}, \ldots, \beta_{s_1}^{(1)})$$

$$- - - - - - - - - - - - - -$$

$$a_n \in F_n = k(\beta_1^{(n)}, \ldots, \beta_{s_n}^{(n)}) \quad ,$$

where all $\beta_j^{(i)} \in F$, so

$$a_1, \ldots, a_n \in k(\beta_1^{(1)}, \ldots, \beta_{s_1}^{(1)}, \ldots, \beta_{s_n}^{(n)})$$

which is linearly disjoint from $k^{1/p}$; hence, $a_1, \ldots, a_n$ satisfy no linear equation over $k^{1/p}$; whence, $k^{1/p}$ and F are linearly disjoint.

Thus in considering linear disjointness it suffices to consider finitely generated subfields.
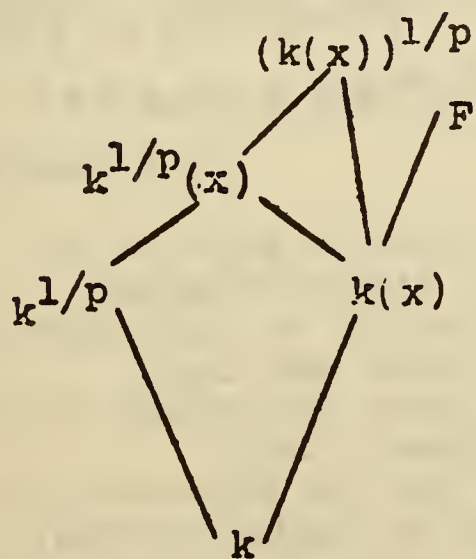
We now introduce an important definition:

Definition 4.1: F is called separably generated (over k) provided F|k is finitely generated, and if F has a transcendence base (x) such that F|k(x) is a separable extension.

Consider, for example, $k(x,y)$ over k where x and y are transcendental elements with $x^2 = y^3 - 1$, and where k is of characteristic two. Then $k(x,y)$ over $k(y)$ is not separable, <u>but</u> $k(x,y)$ over $k(x)$ is separable.

The field $k(x,y)$ over k where x and y are transcendental elements with $x^2 = y^2 + u$ ($u \in k$ and $u \neq s^2$, $s \in k$), and where k is of characteristic two gives an example of a field which is not separably generated. This will be made immediately apparent after the next two theorems.

<u>Theorem 4.3</u>: If F is separably generated over k, then F and $k^{1/p}$ are linearly disjoint over k.

<u>Proof</u>: Let (x) denote a transcendence base of F such that $F/k(x)$ is a separable exten-sion. Then $k(x)$ and $k^{1/p}$ are linearly disjoint over k by Theorem 4.2. Since F is a separable extension of $k(x)$ and finite over $k(x)$, F is generated over $k(x)$ by a primitive element which is separable over $k(x)$. Conse-quently, using Theorem 4.1, we have that $(k(x))^{1/p}$ and F are linearly disjoint over $k(x)$. But $k^{1/p}(x) \subset (k(x))^{1/p}$;

therefore, $k^{1/p}(x)$ and F are linearly disjoint over $k(x)$. Finally, applying lemma 3.2 of the preceding section, we get that F and $k^{1/p}$ are linearly disjoint over k.

Now, we contend that among the finitely generated fields that these are all, i.e., if F/k is finitely generated, and F and $k^{1/p}$ are linearly disjoint over k, then F is separably generated over k. Actually, we will prove even more, namely:

Theorem 4.4: Suppose F is finitely generated over k where F = k(x) ((x) is not necessarily purely transcendental) is a given finite generation. Suppose, also, that F and $k^{1/p}$ are linearly disjoint over k; then F is separably generated, and there exists a subset (y) of (x) such that k(y) is purely transcendental, and F/k(y) is a separable extension.

Proof: If $(x) = (x_1,...,x_n)$ is purely transcendental, then we are, of course, done, so we assume now that algebraic relations are satisfied by them. Let Let $F(X_1,...,X_n) \in k[X]$ be a polynomial of smallest total degree such that $F(x_1,...,x_n) = 0$. Suppose every monomial, v, occurring in F with non-zero coefficients is a p-th power; then F has the form: $\phi(X_1^p,...,X_n^p)$ where

ϕ has lower degree than F. Then

$$\phi^{1/p}(x_1,\ldots,x_n) = 0$$

where $\phi^{1/p}$ has coefficients in $k^{1/p}$. But this means
that a linear relation holds between the monomial values
in the x_1 with coefficients in $k^{1/p}$; hence, by the linear
disjointness, a relation between these monomials holds with
coefficients in k, but this contradicts the fact that F
is the lowest degree equation satisfied by the x_1.
Therefore, some x_1. say x_n, occurs in F with exponents not
all divisible by p. This means that x_n is separable over
$k(x_1,\ldots,x_{n-1})$. Now, either $k(x_1,\ldots,x_{n-1})$ is purely
transcendental: in which case, we are done, or, arguing
as before, we get that, say, x_{n-1} is separable over
$k(x_1,\ldots,x_{n-2})$. Proceeding in this manner, the theorem
is established.

We defined separably generated fields only in the
case where F/k is finitely generated. If F is not
finitely generated over k, we can define it to be sep-
arably generated if and only if every finitely generated
subfield of it is separably generated.

If F is an arbitrary field over k, suppose F is
separably generated; then all finitely generated subfields

F_α are separably generated consequently all F_α and $k^{1/p}$ are linearly disjoint. Conversely, if all F_α and $k^{1/p}$ are linearly disjoint, then all F_α are separably generated, so F is separably generated. Thus F is separably generated if and only if F_α and $k^{1/p}$ are linearly disjoint for all finitely generated subfields F_α of F.

Also we note that if an arbitrary field F is separably generated, then all F_α are separably generated, so all F_α and $k^{1/p}$ are linearly disjoint, hence F and $k^{1/p}$ are linearly disjoint. Conversely, if F and $k^{1/p}$ are linearly disjoint, then all F_α and $k^{1/p}$ are linearly disjoint; whence, all F_α are separably generated, so F is separably generated. Thus Theorem 4.3 and its converse are valid for an arbitrary field F, i.e., not necessarily finitely generated over k.

§5. <u>Fields of definition for an ideal</u>: Let K be a field, and let $\mathcal{U}$ be a proper ideal of K[X]. Then we know that $\mathcal{U}$ has a finite basis in K[X]. We now ask whether or not $\mathcal{U}$ has a basis in k[X] where k is a subfield of K.

<u>Definition 5.1</u>: k is called a field of definition for the ideal $\mathcal{U}$ if $\mathcal{U}$ has a basis in k[X].

In this section, we want to relate the concepts of linear disjointness and field of definition. We first prove the following important theorem:

Theorem 5.1: There is a smallest field of definition.

Proof: $K[X]$ can be viewed as a vector space over K with the set $N = \{v\}$ of all monomials as a basis. $\mathcal{O}$ can also be viewed as a vector space over K, and, consequently, $K[X]/\mathcal{O}$ also can be looked on as a vector space over K. It is certainly generated by N mod $\mathcal{O}$, but this is not a basis for $K[X]/\mathcal{O}$ since certain relations may hold. Let $M = \{\mu\} \subset N$ be a basis mod $\mathcal{O}$ of $K[X]/\mathcal{O}$. For the existence of such a basis, one needs to employ Zorn's Lemma (see, e.g., Jacobson, Lectures in Abstract Algebra, Vol. II, Chapt. IX, Van Nostrand). Now, let $N = M \cup P$ where $P = \{\pi\}$. Suppose $\pi \in P$; then $\pi + \mathcal{O} \in K[X]/\mathcal{O}$. Hence it can be expressed in terms of the basis M of $K[X]/\mathcal{O}$, namely:

$$\pi \equiv \sum_{\mu} a_{\pi,\mu}\mu \qquad (\text{mod } \mathcal{O})$$

with $a_{\pi,\mu} \in K$, and where the representation is unique, and where almost all $a_{\pi,\mu} = 0$ (i.e., all but a finite number equal 0).

Now, let k_0 be the field obtained by adjoining to the prime field **all** such $a_{\pi,\mu}$. We show first that k_0 is a field of definition. Let $f \in \mathcal{U}$; then, since f is a polynomial of $K[X]$, we can write

$$f = \sum_{\pi} b_{\pi}\pi + \sum_{\mu} c_{\mu}\mu$$

where all $b_{\pi}, c_{\mu} \in K$, and where almost all b_{π} and c_{μ} equal 0. Then

$$f = \sum_{\pi} b_{\pi}(\pi - \sum_{\mu} a_{\pi,\mu}\mu) + \sum_{\mu} d_{\mu}\mu,$$

but $f \in \mathcal{U}$, and $(\pi - \sum_{\mu} a_{\pi,\mu}\mu) \in \mathcal{U}$, so $\sum_{\mu} d_{\mu}\mu \in \mathcal{U}$, i.e.,

$$\sum_{\mu} d_{\mu}\mu \equiv 0 \qquad\qquad (\mathrm{mod}\,\mathcal{U}).$$

Since $M \bmod \mathcal{U}$ is a basis of $K[X]/\mathcal{U}$, we get that $d_{\mu} = 0$. Hence,

$$f = \sum_{\pi} b_{\pi}(\pi - \sum_{\mu} a_{\pi,\mu}\mu).$$

Therefore, $\mathcal{U}$ has as a basis all $(\pi - \sum_{\mu} a_{\pi,\mu}\mu) \in \mathcal{U}$ where the coefficients are in k_0 which shows that k_0 is a field of definition. Although all $(\pi - \sum_{\mu} a_{\pi,\mu}\mu)$ do not constitute a finite basis for $\mathcal{U}$, we can easily get a finite subset of them which do constitute a basis by employing the Hilbert Basis Theorem.

Now, let us show that k_o is the smallest field of definition. Suppose k is a field of definition for $\mathcal{O}$, and suppose that $f_1, \ldots, f_r \in k[X]$ constitute a basis for $\mathcal{O}$. Take a $\pi_o \in P$. Then $\pi_o - \sum_\mu a_{\pi_o, \mu} \mu \in \mathcal{O}$, so

$$\pi_o - \sum_\mu a_{\pi_o, \mu} \mu = g_1 f_1 + \ldots + g_r f_r$$

where all $g_i(X) \in K[X]$. Replace each non-zero coefficient b of $g_i(X)$ by an indeterminant, b^*, and denote the corresponding polynomials by $g_i^*(x)$. Then

$$g_1^* f_1 + \ldots + g_r^* f_r = \sum_\pi \lambda_\pi(b^*) \pi + \sum_\mu \lambda_\mu(b^*) \mu$$

where $\lambda_\pi(b^*)$, $\lambda_\mu(b^*)$ are linear functions of the b^* with coefficients in k. Now, consider the system of linear equations

$$\lambda_{\pi_o}(b^*) = 1$$
$$\lambda_\pi(b^*) = 0 \qquad \text{for } \pi \neq \pi_o.$$

This system has a solution $b^* = b$ in K for then each $g_i^* = g_i$. Consequently, it has a solution in k. We denote the solution in k by $\bar{b}$ and the corresponding polynomials by $\bar{g_i}$. Then

$$\bar{g}_1 f_1 + \ldots + \bar{g}_r f_r = \sum_\pi \lambda_\pi(\bar{b})\pi + \sum_\pi \lambda_\mu(\bar{b})\mu$$

$$= \pi_0 + \sum_\mu \lambda_\mu(\bar{b})\mu,$$

but $\bar{g}_1 f_1 + \ldots + \bar{g}_r f_r \in \mathcal{U}$. Thus

$$\pi_0 \cong -\sum_\mu \lambda_\mu(\bar{b})\mu \qquad (\text{mod } \mathcal{U}),$$

and, by the uniqueness of the representation, we get

$$-\lambda_\mu(\bar{b}) = a_{\pi_0,\mu}.$$

Therefore,

$$\bar{g}_1 f_1 + \ldots + \bar{g}_r f_r = \pi_0 - \sum_\mu a_{\pi_0,\mu}\mu,$$

but $\bar{g}_1 f_1 + \ldots + \bar{g}_r f_r \in k[X]$; whence $a_{\pi_0,\mu} \in k$, and this

is true for each π_0, so $k_0 \subset k$ which completes the proof.

We can now easily show that k_0 is finitely gene-
rated over the prime field. Since $\mathcal{U}$ has a finite basis
from $k_0[X]$, let $f_1(X), \ldots, f_\ell(X)$ designate this basis.
Now adjoin to the prime field all the coefficients of the
$f_1(X)$. This gives a field, k_1, which is finitely gene-
rated over the prime field, and where $k_1 \subset k_0$. However,
since k_1 is clearly a field of definition, we must have

$k_1 \supset k_0$. Thus $k_1 = k_0$, and the contention has been established.

Hence, we obtain a refinement of the Hilbert Basis Theorem for $K[X]$; namely, we can obtain a finite basis for an ideal of $K[X]$ where the basis is taken from $k_0[X]$ where k_0 is finitely generated over the prime field.

Let $\mathcal{C} = \mathcal{P}$ be a prime ideal of $K[X]$, and let (x) be a generic point of the variety determined by $\mathcal{P}$. Denote by $\{\bar{v}\}$, $\{\bar{\mu}\}$, $\{\bar{\pi}\}$ the result of substituting (x) for (X) in $\{v\}$, $\{\mu\}$, $\{\pi\}$ respectively. Since $\{\mu\} \bmod \mathcal{P}$ is a basis of $K[X]/\mathcal{P}$, we see that $\bar{\mu}$ is a basis of $K[x]$ over K, and also that

$(5.1) \qquad \bar{\pi} = \sum a_{\pi,\mu} \bar{\mu}.$

Now, let k be a field of definition for $\mathcal{P}$. Then $\mathcal{P} \cap k[X] = \mathcal{Y}$ where $\mathcal{Y}$ is a prime ideal of $k[X]$. But we also have that $\mathcal{P} = \mathcal{Y} K$, for $\mathcal{P}$ has a basis in $k[X]$; therefore, a basis of $\mathcal{P}$ is in $\mathcal{Y}$, and to get an arbitrary element of $\mathcal{P}$, we must form $f_1(X)g_1(X) + \ldots + f_s(X)g_s(X)$ where the $g_i(X) \in \mathcal{Y}$, and the $f_i(X) \in K[X]$. But $f_1(X) = \sum a_v^{(1)} v$, and multiplying $g_1(X)$ by v does not

take us out of $\mathcal{U}$, and multiplying by $a_\nu^{(1)}$ leads into
K $\mathcal{U}$. Therefore, $\mathcal{D} = \mathcal{U}$ K, and, consequently, $\mathcal{U}$ defines
the same variety as $\mathcal{D}$.

Let us now see what a basis of k[x] over k is.
$\{\bar{v}\} = \{\bar{\mu}\} \cup \{\bar{\pi}\}$ will certainly generate k[x] since $\{\bar{v}\}$
gives all monomials, but (5.1) and the fact that all
$a_{\pi,\mu} \in k$ since k is a field of definition show that the
$\bar{\pi}$ are unnecessary. Thus $\{\bar{\mu}\}$ spans k[x] over k, and since
the $\bar{\mu}$ are independent over K, they are independent over k.
Therefore, $\{\bar{\mu}\}$ is a basis of k[x] over k. Hence, K and
k(x) are linearly disjoint since k(x) is the quotient
field of k[x], whose basis stays independent over K.
Thus we've shown:

Theorem 5.2: If k is a field of definition for the
prime ideal $\mathcal{D}$ of K[X], then K and k(x) are linearly
disjoint where (x) is a generic point of the variety
determined by $\mathcal{D}$.

Now let us show that the converse of Theorem 5.2
is true. Let (x) be a point and $\mathcal{D}$ the prime ideal
belonging to it in $\bar{K}[X]$, and let k $\subset$ K be such that K
and k(x) are linearly disjoint. We wish to show that k
is a field of definition for $\mathcal{D}$.

If $\mathscr{Y}$ is the prime ideal belonging to (x) in $k[X]$, then, by the linear disjointness, $\mathscr{D} = \mathscr{Y} K$ which shows that $\mathscr{D}$ has a basis in $k[X]$, namely, that of $\mathscr{Y}$, so k is a field of definition.

Thus we can see the relation between the concepts of linear disjointness and field of definition.

Chapter IV
Projective Varieties

§ 1. Introduction: In this introductory section, we want
to inter-connect the concepts of a homogeneous ideal, a
homogeneous algebraic set, a homogeneous point, and projective
varieties. We denote throughout by k, a given ground field,
and we add a new variable X_o: $(X) = (X_o, X_1, \ldots, X_n)$.

Definition 1.1: $\mathcal{A}$ is called a homogeneous ideal (of k [X])
if every polynomial belonging to it is a sum of homogeneous
polynomials each of which belong to $\mathcal{A}$.

To elaborate a bit further, we associate with each
monomial a degree, namely, if $\mu = X_o^{\mu_o} \ldots X_n^{\mu_n}$, then deg.
$\mu = \mu_o + \ldots + \mu_n$. Then a given polynomial, f, can be written
as $f = \sum_{\nu=o}^{d} f_\nu$ where each term in f_ν is of degree ν. If
$\mathcal{A}$ is homogeneous, and if $f \in \mathcal{A}$, then each f_ν must belong
to $\mathcal{A}$.

We observe, first of all, that the ideal $\mathcal{A}$ is homo-
geneous if and only if $\mathcal{A}$ has a basis consisting of forms
(i.e., homogeneous polynomials). For if $\mathcal{A}$ is homogeneous,
take each member of its finite basis and write it as a sum
of homogeneous polynomials each of which belong to $\mathcal{A}$, so
clearly we get that $\mathcal{A}$ has a basis consisting of forms.
Conversely, let $\mathcal{A} = (f_1, \ldots, f_r)$ where f_1 is a form of
degree d_1. Let $h \in \mathcal{A}$, then $h = g_1 f_1 + \ldots + g_r f_r$. Decom-
pose each g_1 into its homogeneous parts, i.e., $g_1 = \sum_j g_{1j}$

where deg. $g_{ij} = j$. Thus $h = \sum_{i,j} g_{ij}f_i$ where $g_{ij}f_i$ is a

form of degree $j + d_i$. Hence any homogeneous part of h has

the form $\sum g_{ij}f_i \in \mathcal{U}$ where the sum is over those i, j

that give a certain fixed degree, so $\mathcal{U}$ is homogeneous.

We now introduce the next important concept of this

section, namely, that of a homogeneous algebraic set.

<u>Definition 1.2</u>: A is called a homogeneous algebraic set

if $(x) \in A \Longrightarrow (tx) \in A$ for any $t \in \Omega$ where $(tx) =$

$(tx_o, \ldots, tx_n)$.

<u>Theorem 1.1</u>: If $\mathcal{U}$ is a homogeneous ideal, then its associ-

ated algebraic set is a homogeneous algebraic set.

<u>Proof</u>: A basis of $\mathcal{U}$ consists of $f_1, \ldots, f_r$ where each

f_i is a form. The associated algebraic set, A, consists of

the zeros of $\mathcal{U}$. Hence A consists of the set of zeros of the

f_i. If $(x) \in A$, then $f_i(x) = 0$ for each i. Thus $t^{d_i}f_i(x) =$

$0 \Longrightarrow f_i(tx) = 0$ for each i, so $(tx) \in A$.

The converse of Theorem 1.1 is not true unless we

specify the ideal; namely, let A be a homogeneous algebraic

set (possibly not obtained from a homogeneous ideal[*]), and

let $\mathcal{U}$ be the ideal defined by A; then $\mathcal{U}$ is a homogeneous

ideal. To prove this, we let $f \in \mathcal{U}$, and $(x) \in A$. Select

any $t \in \Omega$ such that t is transcendental over $k(x)$. Of course,

---

[*] For example, the ideal $(X_o^3, X_1 + X_o^2)$ determines the alge-

braic set $\{(0)\}$ which is homogeneous, but the ideal is not

homogeneous.

$(tx) \in A$ since A is homogeneous. Now decompose f into its homogeneous parts: $f = \sum_{v=0}^{s} f_v$. Since $f(tx) = 0$, we get that

$$\sum_{v=0}^{s} t^v f_v(x) = 0 ,$$

but this is an equation in t with coefficients from $k(x)$. Consequently, all $f_v(x) = 0$. Thus each f_v vanishes on A since (x) was any point of A; therefore, each $f_v \in \mathscr{a}$ which shows that $\mathscr{a}$ is homogeneous.

The next concept which we want to introduce and to inter-connect with the previous two concepts is that of a homogeneous point.

Definition 1.3: (x) is called a homogeneous point if $(x) \longrightarrow (tx)$ is a specialization for any $t \in \Omega$.

Let $\mathscr{y}$ be the prime ideal determined by (x) where (x) is a homogeneous point. Let $t \in \Omega$ be transcendental over $k(x)$, and let $f \in \mathscr{y}$. Then since $f(x) = 0$, we get that $f(tx) = 0$ which implies that $\sum_{v=0}^{s} t^v f_v(x) = 0$ where $\sum_{v} f_v(x)$ is a decomposition of f into homogeneous parts. Thus we must have $f_v(x) = 0$ for each v, so $f_v \in \mathscr{y}$ for each v which shows that $\mathscr{y}$ is homogeneous, and, consequently, its variety, V, is homogeneous. Thus we've shown that if (x) is a homogeneous point, then the variety of which it is a generic point is homogeneous.

Conversely, let V be a homogeneous variety and (x) a generic point; then $(tx) \in V$ for any $t \in \Omega$ since V is homogeneous; hence, $(x) \longrightarrow (tx)$ is a specialization for any $t \in \Omega$. Thus (x) is a homogeneous point.

Now, suppose that A is a homogeneous algebraic set; we want to see what can be said about its component varieties. Let V be a component of A, and (x) a generic point of V. Let $t \in \Omega$ be transcendental over $k(x)$; then $(tx) \in A$, and (tx) is a generic point of a variety $W \subset A$. Now, we claim that $(tx) \longrightarrow (x)$, i.e., we must show that if $f(tx) = 0$, then $f(x) = 0$. Let $f_\nu = \sum_\nu f_\nu$ be a decomposition of f into homogeneous parts. Then

$$0 = f(tx) = \sum_\nu t^\nu f_\nu(x)$$

which implies that each $f_\nu(x) = 0$, and, therefore, $f(x) = 0$. Thus $(tx) \longrightarrow (x)$, but this means that $V \subset W \subset A$. But V is a component of A, and is, therefore, not contained in any bigger subvariety of A. Hence $V = W$, and (tx) is a generic point of V, and if $\mathcal{Y}$ is the prime ideal determined by (tx), then since $f_\nu(x) = 0$[*] for each ν, we get that $f_\nu(tx) = 0$, so each $f_\nu \in \mathcal{Y}$; whence, $\mathcal{Y}$ is homogeneous, and, therefore, V is homogeneous.

If in the homogeneous space, Ω^{n+1}, we omit the origin and view the __ray__ (tx) as a single point, then we

---

[*] Where $f \in \mathcal{Y}$.

obtain the projective space. A homogeneous variety, so viewed, in the projective space is called a **projective variety**. The dimension of the projective space is one less than that of the homogeneous space.

§ 2. **Solutions of homogeneous problems:** In this section, we want to prove the important theorem due to Hilbert and Zariski which yields necessary and sufficient conditions for certain homogeneous problems to have non-trivial solutions.

Theorem 2.1 (Hilbert-Zariski): Let V be a homogeneous variety, and let A be an algebraic set defined by an ideal $\mathcal{O}\mathcal{l} = (f_1,\ldots,f_r)$ where f_i is a form of deg. $d_i > 0$ (consequently, A is homogeneous). Let (x) be a generic point of V. Then $V \cap A = \{0\}$ if and only if (x) is integral (i.e., each x_i) over $k[f(x)] = k[f_1(x),\ldots,f_r(x)]$.

Proof: Suppose $V \cap A = \{0\}$, but suppose that (x) is not integral over $k[f(x)]$. Thus there exists a place, φ, which is finite on $k[f(x)]$, and, consequently, can be taken as identity on k, but φ is not finite on some x_i. Let $||$ be the valuation associated with φ, and say $\max_i (|x_i|) = |x_n| > 1$. Now

$$(2.1) \qquad \frac{f_i(x)}{x_n^{d_i}} = f_i\left(\frac{x}{x_n}\right)$$

Applying φ to the left side of (2.1), we get 0 since φ is finite on $k[f(x)]$ and since $\varphi(x_n) = \infty$. Applying φ to the right side of (2.1), we get $f_i(\varphi(\frac{x}{x_n}))$, and this can be done since each $|\frac{x_i}{x_n}| \le 1$, and, consequently, φ is finite on each $\frac{x_i}{x_n}$. Hence, we have

$$0 = f_i(\varphi(\frac{x}{x_n}))$$

where $\varphi(\frac{x_i}{x_n}) = \xi_i$ is finite, and we can write $f_i(\xi) = 0$, and this is true for any i. Thus we have found a common zero of these forms which is non-trivial since $\xi_n = 1$. Hence, (ξ) is a non-zero point of A. Furthermore, since (x) is a generic point of the homogeneous variety V we get that $(x) \longrightarrow (\frac{x}{x_n})$ is a specialization, and since φ is finite on each $\frac{x_i}{x_n}$ and a homomorphism on its valuation ring, we get that $(\frac{x}{x_n}) \longrightarrow (\xi)$, so $(x) \longrightarrow (\xi)$. Therefore, $(\xi) \in V$, and we have shown that $(\xi) \in A \cap V$ where (ξ) is non-zero. This gives a contradiction; whence, (x) must be integral over $k[f(x)]$.

Conversely, suppose that (x) is integral over $k[f(x)]$. Then for each i there exists an equation

$$(2.2) \qquad x_i^m + a_{m-1}(f(x))x_i^{m-1} + \ldots + a_0(f(x)) = 0$$

which implies that

(2.3) $\quad X_1^m + a_{m-1}(f(X))X_1^{m-1} + \ldots + a_0(f(X)) \in \mathcal{Y}$

where $\mathcal{Y}$ is the ideal defined by V. $\mathcal{Y}$ is homogeneous; hence, the homogeneous parts of (2.3) belong to $\mathcal{Y}$.

$f_1(X)^{\nu_1} f_2(X)^{\nu_2} \ldots f_r(X)^{\nu_r}$ is a term in the coefficient

of X_1^s; $f_1(X)^{\nu_1} f_2(X)^{\nu_2} \ldots f_r(X)^{\nu_r}$ is a form of degree

$\nu_1 d_1 + \ldots + \nu_r d_r$ which we take equal $m - s$; then

$(f_1(X)^{\nu_1} \ldots f_r(X)^{\nu_r}) X_1^s$ is a form of degree m. We may

therefore, assume that (2.3) is of this form (i.e., homo-
geneous of degree m). That is, we split (2.3) into its
homogeneous components which belong to $\mathcal{Y}$. Take the one
of degree m and call it (2.3). Thus no $a_1(f(X))$ has a
constant term. Now substitute for (X) any $(\xi) \in V \cap A$.
Then the left side of (2.3) becomes equal 0 since $(\xi) \in V$,
and since $(\xi) \in A$, the left side becomes ξ_1^m. Thus we have
$\xi_1^m = 0$, so $\xi_1 = 0$ for any i; hence, $(\xi) = 0$, and the
theorem has been completely established.

Now, let us take the case $V = \Omega^n$ with generic point
$(x) = (x_1, \ldots, x_n)$ where the x_i are algebraically inde-
pendent. Then $V \cap A = A$, so our question becomes whether
$A = (o)$, i.e., whether

$$f_1(X) = 0$$
$$f_2(X) = 0$$
$$- - - - -$$
$$f_r(X) = 0$$

have a common non-trivial solution. From the theorem we
see that they have a common non-trivial solution if (x)
is not integral over $k[f(x)]$. If (x) is not even algebraic
over $k(f(x))$, then (x) certainly cannot be integral over
$k[f(x)]$. If $r < n$, then since the degree of transcendence
of $k(f(x))$ is less or equal r while the degree of trans-
cendence of (x) is n, we see that (x) cannot be algebraic
over $k(f(x))$. Thus we have:

Theorem 2.2: Given a finite number of forms of positive
degree. If there are fewer forms than variables, then the
forms have a common non-trivial zero.

§ 3. Intersection of varieties: We can see clearly that
the dimension of the union of two varieties is equal to the
maximum of the two dimensions. We have previously analyzed
the dimension of subvarieties and the dimension of the pro-
duct of two varieties. It remains for us to analyze the
dimension of the intersection of two varieties. We pro-
pose to do that in this section after extablishing some
preparatory material.

Let (x) be a generic point of the variety V, and

suppose that $(x) \longrightarrow (x')$ is a specialization. The
totality of all $\frac{g(x)}{h(x)}$ where g, h are polynomials of k[x]
and where $h(x') \neq 0$ is called the __local ring__ of the
specialization. Clearly, the local ring of the specializa-
tion $(x) \longrightarrow (x)$ is the whole field k(x). We see further
that any specialization can be extended to its local ring,
and that if we extend the specialization to a place of
the field, then the place is finite on the local ring.

V is called __normal at__ (x') if the local ring, σ,
of $(x) \longrightarrow (x')$ is integrally closed (i.e., integrally
closed in its quotient field). We will also say simply
that (x') __is normal__. V is called __normal__ if it is normal
at each of its points.

__Theorem 3.1:__ Let (x') be normal, and let σ be the local
ring of $(x) \longrightarrow (x')$. Let (y) be __any__ other point such
that (y) is integral over σ. Suppose $(x,y) \longrightarrow (x',y')$, and sup-
pose that $(x) \longrightarrow (\bar{x}) \longrightarrow (x')$. Then there exists a $(\bar{y})$
such that $(x,y) \longrightarrow (\bar{x},\bar{y}) \longrightarrow (x',y')$.

__Proof:__ We observe that (y) is algebraic over k(x), and we
extend k(x,y) to a field K which is normal over k(x) (i.e.,
we go to the splitting field; we note that K|k(x) need not
be a separable extension since k(x) is not necessarily of
characteristic o). Let G be the Galois Group of K|k(x).
$(x) \longrightarrow (\bar{x})$ is a homomorphism of $k[x] \longrightarrow k[\bar{x}] \subset \Omega$.

Extend this to a place $\varphi : K \longrightarrow \Omega \cup \infty$. Let $\sigma \in G$; then $\varphi \sigma$ is also a place of $K \longrightarrow \Omega \cup \infty$, and $x \overset{\sigma}{\longrightarrow} x \overset{\varphi}{\longrightarrow} \bar{x}$. Thus $\varphi \sigma : x \longrightarrow \bar{x}$.

Now, consider the point $(\bar{x}, \varphi \sigma y)$. We must first see if $\varphi \sigma y$ is finite. Let $\frac{g(x)}{h(x)} \in \sigma$; since $h(\bar{x}) = 0 \Longrightarrow h(x') = 0$, we get that $h(x') \neq 0 \Longrightarrow h(\bar{x}) \neq 0$. Thus σ is contained in the local ring of $(x) \longrightarrow (\bar{x})$. Since y is integral over σ, we know that y is integral over the local ring of $(x) \longrightarrow (\bar{x})$. Therefore, σy is also integral over this ring. Since φ is finite on this local ring, and since σy is integral over this local ring, we get that $\varphi \sigma y$ is finite. Hence, we know that $(x, y) \overset{\varphi \sigma}{\longrightarrow} (\bar{x}, \varphi \sigma y)$ is a specialization.

Let us suppose now that for no $\sigma \in G$ will $(\bar{x}, \varphi \sigma y) \longrightarrow (x', y')$ be a specialization. Then for all σ, there exists a polynomial $g_\sigma(X, Y)$ such that $g_\sigma(\bar{x}, \varphi \sigma y) = 0$, but $g_\sigma(x', y') \neq 0$. Let

(3.1)
$$a(X, Y) = \prod_{\tau \in G} (g_\tau(X, Y))^{p^\nu}$$

where p^ν will be chosen large enough to make certain elements, to be introduced presently, separable. If $k(x)$ has characteristic o, we omit the p^ν in (3.1). Now, let us consider $a(x, y)$. For any σ,

$$\varphi \sigma a(x, y) = a(\bar{x}, \varphi \sigma y)$$
$$= \prod_{\tau} (g_\tau(\bar{x}, \varphi \sigma y))^{p^\nu}$$
$$\neq 0$$

114.

since $g_\sigma(\bar{x}, \varphi\sigma y) = 0$, but

$$a(x',y') = \prod_\tau (g_\tau(x',y'))^{p^\nu} \neq 0.$$

Thus, we have that $\varphi\sigma a(x,y) = a(\bar{x}, \varphi\sigma y) = 0$, while $a(x',y') \neq 0$, and from this, we will get a contradiction.

Let τ be any element of G; Then any $\tau a(x,y)$ has the property:

$$\varphi\sigma(\tau a(x,y)) = \varphi(\sigma\tau)a(x,y) = 0$$

Now, let a_1 be an elementary symmetric function of the $\tau a(x,y)$. Then

(3.2) $$\varphi\sigma(a_1) = 0$$

since each $\tau a(x,y)$ has that property. In particular,

(3.3) $$\varphi(a_1) = 0.$$

Since $a(x,y)$ is integral over $\mathscr{o}$, each $\tau a(x,y)$ is integral over $\mathscr{o}$, and, hence, a_1 is integral over $\mathscr{o}$. But $\sigma a_1 = a_1$ for any $\sigma \in G$ which implies that a_1 belongs to the ground field provided it is separable, but a_1 is separable if p^ν is large enough. Consequently, $a_1 \in k(x)$. However, $\mathscr{o}$ is integrally closed in $k(x)$, so we have that $a_1 \in \mathscr{o}$. Thus $a_1 = \dfrac{h_1(x)}{g_1(x)}$ where $g_1(x') \neq 0$, and, therefore, $g_1(\bar{x}) \neq 0$. But, by (3.3),

$$0 = \varphi a_1 = \frac{\varphi h_1(x)}{\varphi g_1(x)} = \frac{h_1(\bar{x})}{g_1(\bar{x})},$$

whence $h_1(\bar{x}) = 0$, which implies that $h_1(x') = 0$. Hence, we know that $a_1(x') = 0$. However, $a(x,y)$ satisfies the equation

$$a^m(x,y) + a_1(x)a(x,y)^{m-1} + \ldots + a_m(x) = 0$$

where $a_1(x) = \dfrac{h_1(x)}{g_1(x)}$. Clearing denominators and noting that $(x,y) \longrightarrow (x',y')$, and that $g_1(x') \neq 0$, we get

$$\mu(x')a(x',y')^m = 0$$

where $\mu(x') \neq 0$, so $a(x',y') = 0$ which gives the desired contradiction and finishes the proof of the theorem.

Before proceeding further, we want to generalize the notion of local ring and obtain some important consequences.

Let R be an integral domain and $\mathscr{y}$ any prime ideal of R. The elements of R not contained in $\mathscr{y}$ form a semigroup (not containing o) which we denote by $S_{\mathscr{y}}$. We form now $\mathscr{v}_{\mathscr{y}}$ which consists of the totality of $\frac{a}{s}$ where $a \in R$, and $s \in S_{\mathscr{y}}$. We will denote $\mathscr{v}_{\mathscr{y}}$ also by $S_{\mathscr{y}}^{-1}R$; $\mathscr{v}_{\mathscr{y}}$ is called the local ring of $\mathscr{y}$. This procedure clearly generalizes what we previously did in the specific case: $R = k[x]$.

We wish to show first that there is a connection between R and certain local rings, namely,

<u>Theorem 3.2</u>: $R = \bigcap_{\mathscr{y}} \mathscr{v}_{\mathscr{y}}$ where $\mathscr{y}$ ranges over the maximal ideals of R.

116.

Proof: 1) Clearly, $R \subset \bigcap_{\mathfrak{p}} R_{\mathfrak{p}}$ since any $a \in R$ can be written as $\frac{a}{1}$ and 1 belongs to all $S_{\mathfrak{p}}$, so $\frac{a}{1}$ belongs to all $R_{\mathfrak{p}}$.

2) Now, suppose that $a \in R_{\mathfrak{p}}$ for all maximal $\mathfrak{p}$. This means that we can write $a = \frac{a_{\mathfrak{p}}}{b_{\mathfrak{p}}}$ where $a_{\mathfrak{p}} \in R$ and $b_{\mathfrak{p}} \notin \mathfrak{p}$ for all maximal $\mathfrak{p}$. Let $\mathfrak{b}$ be the ideal generated by all $b_{\mathfrak{p}}$. We contend that $\mathfrak{b} = R$. If this were not so, then we can find a maximal ideal $\mathfrak{p}_0 \supset \mathfrak{b}$. Hence, on the one hand, $b_{\mathfrak{p}_0} \in \mathfrak{b}$ since $\mathfrak{b}$ is the ideal generated by all $b_{\mathfrak{p}}$, and, on the other hand, $b_{\mathfrak{p}_0} \notin \mathfrak{p}_0$, and, hence $b_{\mathfrak{p}_0} \notin \mathfrak{b}$. Thus $\mathfrak{b} = R$, but $1 \in R$, so there exists $b_{\mathfrak{p}_1}, \ldots, b_{\mathfrak{p}_s}$ and $c_{\mathfrak{p}_1}, \ldots, c_{\mathfrak{p}_s} \in R$ such that

(3.4)
$$1 = c_{\mathfrak{p}_1} b_{\mathfrak{p}_1} + \cdots + c_{\mathfrak{p}_s} b_{\mathfrak{p}_s}.$$

However, $b_{\mathfrak{p}_1} a = a_{\mathfrak{p}_1}$. Multiplying this by $c_{\mathfrak{p}_1}$, and adding over i, and using (3.4), we get

$$a = \sum_{1} c_{\mathfrak{p}_1} a_{\mathfrak{p}_1} \in R,$$

which concludes the proof of the theorem.

Now, let S denote **any** semi-group, not containing o, and contained in R. Then we claim:

Theorem 3.3: If R is integrally closed, then $S^{-1}R$ is integrally closed.

Proof: Let a belong to the quotient field (note: the quotient field of R and $S^{-1}R$ is the same, so there is no ambiguity), and suppose a is integral over $S^{-1}R$. Then a satisfies an equation of the form

$$a^m + \frac{a_1}{s_1}\, a^{m-1} + \ldots + \frac{a_m}{s_m} = 0.$$

Multiplying by $s = s_1 \ldots s_m \in S$, we get

$$sa^m + b_1 a^{m-1} + \ldots + b_m = 0 \, ,$$

and multiplying this by s^{m-1}, we finally get

$$(sa)^m + b_1(sa)^{m-1} + \ldots + b_m s^{m-1} = 0 \, ,$$

which implies that $sa \in R$ since R is integrally closed. Hence $a \in S^{-1}R$.

As a special case of theorem 3.3, we get that if R is integrally closed, then any local ring of $\mathscr{Y}$ is integrally closed.

The converse of theorem 3.3 is true also, but we can prove an even stronger statement, namely: If all $S^{-1}_{\mathscr{Y}} R$ are integrally closed for all maximal $\mathscr{Y}$, then R is integrally closed. For let a belong to the quotient field, and let a be integral over R. Then a is integral over each $S^{-1}_{\mathscr{Y}} R$, so a belongs to each $S^{-1}_{\mathscr{Y}}R$. Hence, using Theorem 3.2, we get that $a \in R$. Thus we can say that R is integrally

118.

closed if and only if each local ring of a maximal ideal
is integrally closed.

Now, let us return to the main considerations of
this section. We recall that a variety, V, was called
normal if it is normal at each of its points. We first want
to show that it suffices to consider only the algebraic
points. To show this, we observe that the algebraic points
correspond to maximal primes, for let (y) be a generic
point of V and let (x) be any algebraic point of V. Let
$\wp_y$ and $\wp_x$ be the corresponding prime ideals. Then $\wp_y \subset \wp_x$.
Suppose there exists a $\wp^*$ such that $\wp_y \subset \wp_x \subset \wp^*$; let
$\wp_x \longrightarrow V_x$ and $\wp^* \longrightarrow V^*$. Then $V \supset V_x \supset V^*$ and $(y) \longrightarrow (x) \longrightarrow (z)$
where z is a generic point of V^*, so $f(x) = 0$ implies that
$f(z) = 0$, but if $\wp_x \subset \wp^*$ properly, then there exists a $g \in \wp^*$,
but $g \notin \wp_x$, i.e., $g(z) = 0$ but $g(x) \neq 0$. However, this is a
contradiction, for since (x) is algebraic, every specializa-
tion is an equivalent generic point. Now, a variety V, with
generic point (x) is normal at each of its algebraic points if
and only if the associated local rings are integrally closed,
but, by the remarks after Theorem 3.3, and by the previous
remarks, this is true if and only if $R = k[x]$ is integrally
closed, in which case V is then normal at all of its points
by Theorem 3.3.

We wish to show now that the entire space $V = \Omega^n$
is normal. Let $(x) = (x_1, \ldots, x_n)$ where the x_i are alge-
braically independent be a generic point. To show that

Ω^n is normal, we must just show that $k[x]$ is integrally
closed. But $k[x]$ is just the polynomials in n variables,
and, therefore, a unique factorization ring. However, any
unique factorization ring is integrally closed, for let
$\frac{p}{q} = a \in k(x)$, where $p, q \in k[x]$ and where we may assume
that p and q are relatively prime since $k[x]$ is an unique
factorization domain. Now suppose that a satisfics the
equation

$$a^n + a_1 a^{n-1} + \ldots + a_n = 0$$

where all $a_i \in k[x]$. Then we have

$$p^n + a_1 p^{n-1} q + \ldots + a_n q^n = 0.$$

Let π be a prime such that π/q; then π/p^n, which implies
that π/p since we are in a domain of unique factorization,
but this contradicts the fact that p and q are relatively
prime. Hence, it follows that no prime divides q, so q is
a unit. Thus $a = pq^{-1} \in k[x]$.

Consequently, $k[x]$ is integrally closed, and Ω^n is
normal.

If (x) is a generic point of V where the x_i are
algebraically independent, then, as we've just seen $k[x]$
is integrally closed whence V is normal; in particular, it
is normal at (x') where $(x) \longrightarrow (x')$. Also, let (y) be
integral over $k[x]$; then (y) is certainly integral over the
local ring of $(x) \longrightarrow (x')$. Thus, by Theorem 3.1, we
can say: If (x) is such that all x_i are algebraically
independent, and if (y) is integral over $k[x]$, then if

$(x,y) \longrightarrow (x',y')$, and if $(x) \longrightarrow (\bar{x}) \longrightarrow (x')$, then there exists a $(\bar{y})$ such that $(x,y) \longrightarrow (\bar{x},\bar{y}) \longrightarrow (x',y')$.

Let the ideal $(f_1,\ldots,f_r)$ determine the algebraic set A. Instead of writing $V \cap A$ where V is some variety, we will also write $V \cap (f_1,\ldots,f_r)$ (i.e., V intersect the algebraic set determined by $(f_1,\ldots,f_r)$).

Now, let A be an algebraic set, and let $\mathscr{Y}_1, \ldots, \mathscr{Y}_s$ be the prime ideals belonging to the component varieties of A. If A is a homogeneous algebraic set, then each $\mathscr{Y}_1$ is homogeneous since, as we've seen, each component of a homogeneous algebraic set is homogeneous. Also, we note that there are no inclusion relations between the $\mathscr{Y}_1$. We wish to show that there exists a polynomial (form of positive degree in the case where A is homogeneous) not contained in any of the $\mathscr{Y}_1$. To do this, we first note that

$$\mathscr{Y}_1 \mathscr{Y}_2 \cdots \mathscr{Y}_{i-1} \mathscr{Y}_{i+1} \cdots \mathscr{Y}_s \not\subset \mathscr{Y}_i ,$$

for select $\pi_1 \in \mathscr{Y}_1$, and $\pi_1 \notin \mathscr{Y}_i$; $\pi_2 \in \mathscr{Y}_2$, and $\pi_2 \notin \mathscr{Y}_i$, etc. Then

$$\pi_1 \pi_2 \cdots \pi_{i-1} \pi_{i+1} \cdots \pi_s \in \mathscr{Y}_1 \cdots \mathscr{Y}_{i-1} \mathscr{Y}_{i+1} \cdots \mathscr{Y}_s ,$$

and

$$\pi_1 \pi_2 \cdots \pi_{i-1} \pi_{i+1} \cdots \pi_s \notin \mathscr{Y}_i$$

since $\mathscr{Y}_i$ is a prime ideal.

Now select $g_i \in \mathcal{Y}_1 \cdots \mathcal{Y}_{i-1} \mathcal{Y}_{i+1} \cdots \mathcal{Y}_s$ such that $g_i \notin \mathcal{Y}_i$. If A is homogeneous, g_i can be s lected as a form of positive degree, since we can make $\pi_1, \pi_2, \ldots$ forms since the $\mathcal{Y}_i$ are generated by forms. g_i has the property of being in each $\mathcal{Y}_j$ for $j \neq i$ and not in $\mathcal{Y}_i$. Let $f = \sum g_i^{\mu_i}$ (where μ_i is chosen so as to make f a form in the case where A is homogeneous). Then $f \notin \mathcal{Y}_i$ for any i, since f is a sum of terms all of which are in $\mathcal{Y}_i$ except one. We observe that the previous proof goes through provided that we have at least two prime ideals. If there is only one prime ideal, then the contention is clearly true except in the case in which the variety of this prime is (o), for then every form of positive degree is contained in the prime ideal.

Now, let V_i be the variety of $\mathcal{Y}_i$; then $f \notin \mathcal{Y}_i$, for any i, implies that $V_i \not\subseteq (f)$, for any i, where (f) denotes, now, the algebraic set determined by the ideal (f). Thus we have that $\dim (A \cap (f)) < \dim A$.

This result will help us in establishing the following theorem:

Theorem 3.4: Let V be a homogeneous variety, and suppose $\dim V = r$, then each component of $(V \cap (f))$ has dimension greater than or equal $r-1$ where f is a form of positive degree.

Proof: We must prove if $\dim V = r$, and if f is a form of positive degree, then each component of $V \cap (f)$ has dimension

greater than or equal r-1. Hence, we may assume that $V \not\subset (f)$, for if $V \subset (f)$, the dimension statement is trivial.

Then dim $(V \cap (f)) \leq r-1$. By our previous result, we know that we can find a form, f_2, of positive degree such that dim $((V \cap (f)) \cap (f_2)) \leq r-2$. Continuing in this manner, we get that there exists forms of positive degree: f_2, f_3, ... f_s, where $s \leq r$, such that

$$\dim (V \cap f \cap f_2 \cap ... \cap f_s) = 0,$$

setting $f = f_1$, we have that

$$V \cap (f_1, f_2, ..., f_s) = (0),$$

since $V \cap (f_1, f_2, ..., f_s)$ is a homogeneous algebraic set, so if it contained a point $(x) \neq (0)$, then it would contain the whole ray (tx), for any $t \in \Omega$, and, consequently, would have dimension greater than 0. We also note that we can't go below dimension 0 by our previous remarks in establishing the existence of $f \not\subset \mathcal{J}_1$, for any i.

We now want to show that we actually need r steps, i.e., $s = r$. Applying Theorem 2.1 of this chapter, we get that (x) is integral over $k[f_1(x), ..., f_s(x)]$, where (x) is a generic point of V. This, of course, implies that (x) is algebraic over $k(f_1(x), ..., f_s(x))$. But dim $(x) = r$; therefore, the degree of transcendence of $k(f_1(x), ..., f_s(x))$ over k is greater than or equal r,

so $s \geq r$. Thus $s = r$. Hence, we need r steps, so
dim $(V \cap (f))$ is at least $r - 1$, which tells us that at
least one component of $V \cap (f)$ has dimension at least
$r - 1$. We must show, however, that this is true for each
component.

Let us recapitulate what has been done so far. Let
$f = f_1$, and let (x) be a generic point of V. We have ob-
tained forms of positive degree: $f_1, \ldots, f_r$ such that

$$V \cap (f_1, \ldots, f_r) = (0).$$

We then know that (x) is integral over $k[y]$ where $y_1 = f_1(x)$ $i = 1, \ldots, r$. Since dim $(x) = r$, and since (x)
is algebraic over $k(y)$, we know that dim$(y) \geq r$. Hence
dim $(y) = r$. Thus the y_1 are algebraically independent.

Now let $(p) \in V \cap (f_1)$, i.e., $(x) \longrightarrow (p)$, and
$f_1(p) = 0$. Consider the point (y,x) where $(y) = (f(x))$.
Then $(y,x) \longrightarrow (f(p),p)$ since $(x) \longrightarrow (p)$ is a speciali-
zation which sends $f(x) \longrightarrow f(p)$. Hence, $(y) \longrightarrow (f(p))$
(This also follows from the fact that the y_1 are alge-
braically independent). Let $(\bar{y}) = (0, y_2, \ldots, y_r)$; then
$(y) \longrightarrow (\bar{y}) \longrightarrow (f(p))$ since the $y_2, \ldots, y_r$ are alge-
braically independent, and since $f_1(p) = 0$. Thus we know
that there exists an $(\bar{x})$ such that $(y,x) \longrightarrow (\bar{y}, \bar{x}) \longrightarrow$
$(f(p),p)$. Since $(y) = (f(x))$, we have $(\bar{y}) = (f(\bar{x}))$, but
$\bar{y}_1 = 0$, so $f_1(\bar{x}) = 0$. This means that $(\bar{x}) \in (f_1)$. We also

have that $(x) \longrightarrow (\bar{x})$ since $(y,x) \longrightarrow (\bar{y},\bar{x})$. Hence, $(\bar{x}) \in V$, and, therefore, $(\bar{x}) \in V \cap (f_1)$.

From $(\bar{y}) = (f(\bar{x}))$, we get

$$r-1 = \dim (\bar{y}) \leq \dim (\bar{x}),$$

so $\dim (\bar{x}) \geq r-1$. Thus we have constructed an $(\bar{x})$ such that $(\bar{x}) \in V \cap (f_1)$, and $\dim (\bar{x}) \geq r-1$. Since $(\bar{x}) \longrightarrow (p)$, (p) is a point of the variety of which $(\bar{x})$ is the generic point. Consequently, every point of $V \cap (f_1)$ lies in a variety of at least dimension $r-1$, which finally completes the proof of Theorem 3.4.

Before considering the general problem of the intersection of any two varieties, we must consider more closely the connection between the varieties we originally considered — affine varieties — and the varieties introduced in this chapter — homogeneous varieties.

Let $X = (X_1, \ldots, X_n)$, and let $\mathscr{S} = k[X]$, and $\mathscr{U} = k[X_0, X]$. With a polynomial $f \in \mathscr{S}$, we will associate a form $f^* \in \mathscr{U}$ in the following way: let $d = \deg f$; then

$$X_0^d f\left(\frac{X}{X_0}\right) = f^*(X_0, X)$$

is a form.

Now, let g be a form of $\mathscr{U}$. We will associate with g a polynomial $g' \in \mathscr{S}$ as follows:

$$g'(X) = g(1,X).$$

It is clear that $(f^*)' = f$, but the reverse procedure is not true; namely, suppose that f is a form of degree d. Then $f'(X) = f(1,X)$ is of degree $d' \le d$. Hence

$$(f')^* = X_0^{d'} f(1, \frac{X}{X_0})$$

$$= X_0^{d'-d} f(X_0, X).$$

Let $\mathcal{M}$ be an ideal of $\mathcal{U}$; then $\mathcal{M}^*$ shall be the ideal in $\mathcal{U}$ generated by those forms f for which $f' \in \mathcal{M}$.

If (x) is any zero of $\mathcal{M}$, and $t \in \Omega$, then (t,tx) is a zero of $\mathcal{M}^*$. To prove this, it suffices to show that (t,tx) is a zero of the generators of $\mathcal{M}^*$. If f is one of the generators, then $f' \in \mathcal{M}$, so

$$f(t,tx) = t^d f(1,x)$$

$$= t^d f'(x)$$

$$= 0.$$

Now suppose that (x_0,x) is a zero of $\mathcal{M}^*$ and that $x_0 \ne 0$. If $f \in \mathcal{M}$, then $f^* \in \mathcal{M}^*$, since $(f^*)' = f \in \mathcal{M}$. Hence,

$$0 = f^*(x_0,x) = x_0^d f(\frac{x}{x_0})$$

which implies that $\frac{x}{x_0}$ is a zero of $\mathcal{M}$.

We now suppose that V is an affine variety (i.e., V consists of the zeros of a prime ideal $\mathcal{Y}$ of $\mathcal{U}$) of dimension r and with generic point (x). Take $t \in \Omega$

and t algebraically independent over $k(x)$. We wish to show that (t, tx) is a generic point of V^* where $\mathcal{Y}^* \longrightarrow V^*$. Let $\widetilde{\mathcal{Y}}$ be the prime ideal of $\mathcal{Y}$ belonging to (t, tx). We must show that $\widetilde{\mathcal{Y}} = \mathcal{Y}^*$.

1) Since, by the preceding discussion, $(t, tx) \in V^*$, we get that $\mathcal{Y}^* \subset \widetilde{\mathcal{Y}}$.

2) $\widetilde{\mathcal{Y}}$ is homogeneous. For let $F \in \widetilde{\mathcal{Y}}$, and let $F = \sum_{\nu} F_{\nu}$ be a decomposition of F into homogeneous parts of degree ν. Then

$$0 = F(t, tx) = \sum_{\nu} t^{\nu} F_{\nu}(1, x),$$

which implies that each $F_{\nu}(1, x) = 0$, so, multiplying by t^{ν}, we get that each $F_{\nu}(t, tx) = 0$. But this means that all $F_{\nu} \in \widetilde{\mathcal{Y}}$, so $\widetilde{\mathcal{Y}}$ is homogeneous. Hence, to show that $\widetilde{\mathcal{Y}} \subset \mathcal{Y}^*$, we must just show that if f is a form of $\widetilde{\mathcal{Y}}$, then $f \in \mathcal{Y}^*$. Now, $f \in \widetilde{\mathcal{Y}}$ where f is a form means that $f(t, tx) = 0$. This implies that $f(1, x) = 0$, so $f'(x) = 0$. Hence, $f' \in \mathcal{Y}$, whence $f \in \mathcal{Y}^*$.

Thus to an affine variety, V, of dimension r and generic point (x), there corresponds a homogeneous variety V^*, with generic point (t, tx) and of dimension $r + 1$. Viewed as a projective variety, V^* has the same dimension as V since the dimension of the projective variety is one lower than that of the homogeneous variety.

Let V be an affine variety of dimension r, and

suppose that $f \in \mathscr{r}$. We must make the added assumption, which was not needed in the homogeneous case, that $V \cap (f) \neq \phi$. Suppose $(p) \in V \cap (f)$. Then $(t,tp) \in V^{\#}$ for $t \in \Omega$, so $(1,p) \in V^{\#}$, and $(1,p) \in (f^{\#})$, since $f^{\#}(1,p) = f^{\#'}(p) = f(p) = 0$. Also, note that $f^{\#}$ is a form. Applying Theorem 3.4, we get that there exists a point $(x_0,x) \in V^{\#} \cap (f^{\#})$ such that $\dim (x_0,x) \geq r$, and such that $(x_0,x) \longrightarrow (1,p)$. Since $x_0 \neq 0$, we have that $(\frac{x}{x_0}) \in V$, and $f(\frac{x}{x_0}) = x_0^{-d} f^{\#}(x_0,x) = 0$. Thus $(\frac{x}{x_0}) \in V \cap (f)$, and $\dim (\frac{x}{x_0}) \geq r-1$. Furthermore, $(\frac{x}{x_0}) \longrightarrow (p)$, so we obtain Theorem 3.4 in the case of affine varieties with the added assumption that $V \cap (f) \neq \phi$.

Finally, let us consider the general case of the intersection of any two varieties. Let V and W be varieties in Ω^n with $\dim V = r$ and $\dim W = s$. Then $V \times W$ is an algebraic set of Ω^{2n}, and is of dimension $r+s$ in each component. Let (x) be a point of V and (y) a point of W; then $(x,y) \in V \times W$. Ω^{2n} consists, of course, of the totality of points $\{(x_1,\ldots,x_n,y_1,\ldots,y_n)\}$ where $x_i,y_j \in \Omega$. Let $\triangle$ be the diagonal set in Ω^{2n}; i.e., $\triangle$ consists of the totality of elements of Ω^{2n} of the form $\{(x_1,\ldots,x_n,x_1,\ldots,x_n)\}$. $\triangle$ is an algebraic set determined by the ideal

$$(f_1 = X_1 - Y_1, \quad f_2 = X_2 - Y_2, \quad \ldots\ldots, \quad f_n = X_n - Y_n).$$

Now, $(V \times W) \cap \triangle = \{(x,x) \mid (x) \in V \text{ and } (x) \in W\}$, i.e., $(V \times W) \cap \triangle = \{(x,x) \mid (x) \in V \cap W\}$.

Applying our previous result n times, we get that
the dimension of $(V \times W) \cap \triangle$ is greater than or equal
$r + s - n$ in each component; whence each component of $V \cap W$
has dimension greater than or equal $r + s - n$, so

(3.5) $\dim(V \cap W) \geq r + s - n$

provided that $V \cap W \neq \phi$.

This result is also true for homogeneous varieties,
since the case of homogeneous varieties is just a special
case of this, and, for homogeneous varieties, we need no
added condition since they always intersect; namely, they
always have (o) in common.

Now, let V and W be projective varieties of dimensions
r and s respectively. The corresponding homogeneous varieties
have dimensions $r + 1$, $s + 1$ respectively, and the whole
space dimension $n + 1$. Applying (3.5) to these homogeneous
varieties, we get that their intersection has dimension
$\geq (r+1) + (s+1) - (n+1) = r+s - n+1$ in each component. Going
back now to the projective variety, we get the desired result
for projective varieties. Thus (3.5) is true for projective
varieties if it is significant, i.e., in projective space,
if the right side of (3.5) is significant, then the two
projective varieties intersect, and (3.5) gives the rele-
vant information concerning the dimension of the inter-
section.

Chapter V

Applications to Elimination Theory

§ __Introduction__: We now want to apply some of the results
which we've obtained to elimination theory. We note that
the procedure could be reversed; namely, one can obtain
results in elimination theory independently of results in
algebraic geometry, and then apply these results to alge-
braic geometry.

The central problem in elimination theory is to
determine what conditions must be put on the coefficients
so that a number of forms have a non-trivial solution.

Thus, let us assume that we are given positive integers
d_1, d_2, ..., d_r. Let f_1, f_2,....,f_r be forms of degree
d_1, d_2,...., d_r, and, finally, let X_1, X_2, ..., X_n be the
variables of the forms. Denote the coefficients of

$$f_1 \text{ by } (a')$$

$$f_2 \text{ by } (b')$$

$$\cdots\cdots\cdots$$

$$f_r \text{ by } (e')$$

We now view the forms as given by a point $(a', b', ..., e')$
in a space of dimension N (where N equals the sum of the
number coefficients of all the forms). We take the subset
of the totality of all $(a', b', ..., e')$ such that the

related forms have a non-trivial common solution. We wish to show that this subset forms a variety. To demonstrate this, we will obtain a generic point.

We pick one of the X_1, say X_n, and write

$$f_1(X) = a_n X_n^{d_1} + f_1^*(X)$$

$$f_2(X) = b_n X_n^{d_2} + f_2^*(X)$$

$$\cdots \cdots \cdots \cdots$$

$$f_r(X) = e_n X_n^{d_r} + f_r^*(X).$$

We will denote the coefficients of f_1^*, f_2^*, ..., f_r^* by (a), (b), ..., (e). We replace (a'), (b'), ..., (e') by (a_n, a), (b_n, b), ..., (e_n, e) so that our point in the space of dimension N is now $(a_n, a, b_n, b, ..., e_n, e)$. Select a, b, ..., e algebraically independent over k, and choose $(x) = (x_1, ..., x_n)$ algebraically independent over $k(a, b, ..., e)$. Then the desired generic point will be

$$P_n = (-\frac{f_1^*(x)}{x_n^{d_1}}, a, -\frac{f_2^*(x)}{x_n^{d_2}}, b, ..., -\frac{f_r^*(x)}{x_n^{d_r}}, e)$$

We note, before proving the above assertions, that we could have singled out any one of the variables other than X_n. This procedure would lead to equivalent generic points P_1.

To prove the preceding assertions, we show first that the forms with the coefficients

$$(-\frac{f_1^*(x)}{x_n^{d_1}}, \; a, \; \ldots, \; -\frac{f_r^*(x)}{x_n^{d_r}}, \; e) = P_n \text{ have a common non-}$$

trivial solution. This is clear since

$$f_1 = -\frac{f_1^*(x)}{x_n^{d_1}} X_n^{d_1} + f_1^*(X)$$

$$f_2 = -\frac{f_2^*(x)}{x_n^{d_2}} X_n^{d_2} + f_2^*(X)$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$f_r = -\frac{f_r^*(x)}{x_n^{d_r}} X_n^{d_r} + f_r^*(X)$$

have $(X) = (x) \neq (0)$ as a common solution.

Now, we must show that if $Q = (\bar{a}_n, \; \bar{a}, \; \bar{b}_n, \; \bar{b}, \ldots, \; \bar{e}_n, \; e)$ is a system of forms

$$\bar{f}_1 = \bar{a}_n X_n^{d_1} + \bar{f}_1^*(X)$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\bar{f}_r = \bar{e}_n X_n^{d_r} + \bar{f}_r^*(X)$$

which has a common non-trivial solution $(\bar{x})$, then $P_n \longrightarrow Q$. To prove this, we assume, at first, that $\bar{x}_n \neq 0$. Then, by assumption,

$$\bar{a}_n \bar{x}_n^{d_1} + \bar{f}_1^*(\bar{x}) = 0$$

$$\cdots\cdots\cdots\cdots\cdots$$

$$\bar{e}_n \bar{x}_n^{d_r} + \bar{f}_r^*(\bar{x}) = 0,$$

132.

so

$$\bar{a}_n = -\frac{\bar{f}_1^*(\bar{x})}{\bar{x}_n^{d_1}}, \ldots, \bar{e}_n = -\frac{\bar{f}_r^*(\bar{x})}{\bar{x}_n^{d_r}}. \quad \text{Hence,}$$

$$Q = (-\frac{\bar{f}_1^*(\bar{x})}{\bar{x}_n^{d_1}}, \bar{a}, \ldots, -\frac{\bar{f}_r^*(\bar{x})}{\bar{x}_n^{d_r}}, \bar{e}).$$

Now, $(x, a, b, \ldots, e) \rightarrow (\bar{x}, \bar{a}, \bar{b}, \ldots, \bar{e})$ is certainly a specialization since $(x, a, \ldots, e)$ are algebraically independent. However, this specialization induces $P_n \rightarrow Q$, which is the contention provided $\bar{x}_n \neq 0$.

In particular, we get $P_n \rightarrow P_i$ for all i. Since Q yields forms having a non-trivial solution, some $\bar{x}_i \neq 0$. Then $P_i \rightarrow Q$, so $P_n \rightarrow Q$, and the contention has been completely established.

Finally, we must show that if Q is a specialization of P_n that then Q comes from a set of forms with a common non-trivial solution. To prove this, we will simply show that if a certain system of forms has a common non-trivial solution, then specializing the related point leads to forms with common non-trivial solutions.

Thus, suppose that P gives a system of forms f_i $i = 1, \ldots, r$ which has a common non-trivial zero, (ξ): $f_i(\xi) = 0$, $i = 1, \ldots, r$. Let $P \rightarrow Q$, and let $\bar{f}_i$ be the forms belonging to Q. We want to show that the $\bar{f}_i$ have a common non-trivial zero. We extend the homomorphism $P \rightarrow Q$ to a place ϕ applicable to ξ. Denote by $\| \|$ the associated

valuation. Assume that $|\xi_n| \geq |\xi_1|$ for all i. Then

$$f_1(\xi) = 0 \Rightarrow \frac{1}{\xi_n^{d_1}} f_1(\xi) = 0 \Rightarrow f_1(\frac{\xi}{\xi_n}) = 0. \quad \text{Since } |\frac{\xi_1}{\xi_n}| \leq 1,$$

we can apply ϕ to $f_1(\frac{\xi}{\xi_n})$; therefore,

$$\bar{f}_1(\phi(\frac{\xi}{\xi_n})) = 0 \qquad \text{for all i.}$$

Thus we have obtained a common solution of the $\bar{f}_1$, which is non-trivial since $\phi(\frac{\xi_n}{\xi_n}) = \phi(1) = 1$.

Combining the previous results, we now have that the points of this space of dimension N which lead to forms having a common non-trivial solution form a variety with P_n as a generic point.

Since $f_1^*(x)$ is a form of degree d_1, we have $\dfrac{f_1^*(x)}{x_n^{d_1}} = f_1^*(\frac{x}{x_n})$. Now,

$$(\frac{x}{x_n}) = (\frac{x_1}{x_n}, \frac{x_2}{x_n}, \ldots, \frac{x_{n-1}}{x_n}, 1)$$

$$= (y_1, y_2, \ldots, y_{n-1}, y_n = 1)$$

$$= (y)$$

where $y_1, y_2, \ldots, y_{n-1}$ are algebraically independent over $k(a, b, \ldots, e)$. Therefore, we can say that P is a generic point of the variety where

$$P = (-f_1^*(y), a, -f_2^*(y), b, \ldots, -f_r^*(y), e),$$

and dim $P \leq N - r + s$ where $s = \text{Min } (r, n-1)$.

We contend that this is the precise dimension.

Thus, we have to prove that dim $P \geq N - r + s$; i.e., we
must show that, say, $f_1^*(y)$, $f_2^*(y)$, .., $f_s^*(y)$ ($s = \text{Min}(r, n-1)$)
are algebraically independent over $k(a, b, .., e)$. To this end,
we prove:

<u>Lemma 1.1</u>: Let (a) denote elements which are algebraically
independent over k, and let (y) be algebraically independent
over $k(a)$. Furthermore, let $g_1(y)$, $g_2(y)$, ..., $g_s(y)$ ($s \leq n-1$)
be polynomials whose coefficients are in $k[a]$. Suppose there
is a non-zero polynomial $\phi(X, Y) \in k[X, Y]$ such that
$\phi(a, g(y)) = 0$. Then if one of the coefficients a_1 is special-
ized to $a \in k$, and if $\bar{g}(y)$ is the corresponding specialization
of $g(y)$, and if, furthermore, (a') are the remaining co-
efficients (which are not specialized), then there exists a
polynomial, $\psi \neq 0$, such that $\psi(a', \bar{g}(y)) = 0$.

<u>Proof</u>: Write $\phi(X, Y) = \phi(X', X_1, Y)$.
Then
$$\phi(a', a_1, g(y)) = 0;$$
hence,
$$\phi(a', a, \bar{g}(y)) = 0,$$

so it would seem that $\psi = \phi(X', a, Y)$ is the desired poly-
nomial, but it is possible that $\phi(X', a, Y)$ is identically
zero. If $\phi(X', a, Y)$ is zero, then $\phi(X', X_1, Y)$ has the factor
$X_1 - a$. We write
$$\phi(X', X_1, Y) = (X_1 - a)^m \psi(X', X_1, Y)$$

where m is maximal. Then, since $\phi(a', a_1, g(y)) = 0$, we
have

$$(a_1 - a)^m \psi(a', a_1, g(y)) = 0$$

but $(a_1-a) \neq 0$ since a_1 is algebraically independent over k, while $a \in k$. Thus

$$\psi(a', a_1, g(y)) = 0 ,$$

so

$$\psi(a', a, \bar{g}(y)) = 0 ,$$

and $\psi(X', a, Y) \neq 0$, so ψ is the required polynomial.

Now, if $f_1^*(y)$, $f_2^*(y)$, ..., $f_s^*(y)$ $(s \leq n-1)$ were algebraically dependent over $k(a,b,\ldots,e)$, then special-izing

$$f_1^*(y) \text{ to } y_1^{d_1}$$
$$f_2^*(y) \text{ to } y_2^{d_2}$$
$$\cdots \cdots \cdots$$
$$f_s^*(y) \text{ to } y_s^{d_s} \qquad (s \leq n-1) ,$$

we would obtain by repeated applications of the lemma that $y_1^{d_1},\ldots, y_s^{d_s}$ $(s \leq n-1)$ are algebraically dependent over k which is a contradiction. Thus dim $P = N-r+s$, and our variety is of dimension $N-r+s$.

We define the <u>codimension</u> of a point or variety as N minus the dimension of the point or variety, so codim $P = r-s$, and the codimension of our variety is $r-s$.

If $r \leq n-1$, then $s = r$, and codim $P = 0$, so our variety is then the whole space, and we have another proof of Theorem 2.2 of Chapter IV.

If $r \geq n$, then $s = n-1$, and codim $P = r-n+1$. In particular, if $r = n$, then codim $P = 1$, and our variety

is a hypersurface. Hence, in this case, there exists an irreducible polynomial in the coefficients of f_1, f_2,.., f_n which we denote by $R_k(f_1, .., f_n)$, and which is determined up to a factor of k, such that $R_k(\bar{f}_1, .., \bar{f}_n) = 0$ (where $\bar{f}_1, .., \bar{f}_n$ are specialized forms) is a necessary and sufficient condition for

$$\bar{f}_1 = 0$$
$$\bar{f}_2 = 0$$
$$\cdots\cdots$$
$$\bar{f}_n = 0$$

to have a common non-trivial solution. R_k is called the __resultant__ of the n forms. If there are more forms than variables, then we get more than one resultant since a variety consists of the points annihilating an ideal.

We note that in the case of linear equations R_k is the determinant.

Now, we write $f_n = e_n X_n^{d_n} + f_n^*(X)$; we contend that R_k depends on e_n (similarly, on a_n, b_n, ...). For suppose it did not depend on e_n. Since R_k must vanish for our generic point P (r = n now), this would mean that $f_1^*(y), .., f_{n-1}^*(y)$ are dependent over k(a, b, .., e), but we've already seen that this can't happen.

Let $\bar{f}_1, .., \bar{f}_r$ have a common non-trivial zero. Then multiplying $\bar{f}_1$ by any element λ, we see that $\lambda\bar{f}_1$ has the

same zero. Similarly, $\mu \bar{f}_2$ where μ is any element has the same zero, etc. But this means that our variety is multiple homogeneous; i.e., it is

homogeneous in the coefficients of f_1

          "   "   "   "   " f_2

   . . . .

         "   "   "   "   " f_r

(i.e., homogeneous in each separately).

Now, we can duplicate the proofs we did in Chapter IV for homogeneous varieties in the case of multiple homogeneous varieties. Instead of forms, we would now take multiforms, i.e., polynomials in (a'), (b'), .., (e') which are homogeneous in (a'), (b'), .., (c') separately. We would then get that if a variety is multiple homogeneous, then, its defining ideal is generated by multi-forms. Thus we get that the resultant is a multi-form, or, as we will also say, a multiple homogeneous polynomial.

§ 2. <u>The resultant of n forms</u>: We want now to give a method, at least in principle, for calculating R_k. We know that R_k is homogeneous in (e'). We will show that it is homogeneous of degree $d_1 d_2 \ldots d_{n-1}$ in (e'). Similarly, it is homogeneous of degree $d_2 d_3 \ldots d_n$ in (a'), homogeneous of degree $d_1 d_3 \ldots d_n$ in (b'), etc.

Let $d_1 = d_1' + d_1''$, and let g_1 be a generic form (i.e., with general coefficients) of degree d_1' and h_1 a generic form of degree d_1'' . Put $\bar{f}_1 = g_1 h_1$, and suppose that $\bar{f}_1$ is

a specialization of f_1 (i.e., specialized coefficients of f_1). We want to see if there is a relationship between $R_k(\bar{f}_1, f_2, .., f_n)$ and $R_k(g_1, f_2, .., f_n)$. Let $\left\{R_k(f_1, f_2, .., f_n)\right\}$ (i.e., the generated ideal) determine the variety V, and $\left\{R_k(g_1, f_2, ..., f_n)\right\} <\to> \ddot{V}$. If $(\xi) \in \ddot{V}'$, then for this (ξ), $R_k(\ddot{g}_1, \hat{f}_2, .., \hat{f}_n) = 0$; i.e., $\hat{g}_1 = 0$, $\hat{f}_2 = 0$, .., $\hat{f}_n = 0$ have a common non-trivial solution, so $\bar{\hat{f}}_1 = 0$, $\hat{f}_2 = 0, ..., \hat{f}_n = 0$ have a common non-trivial solution. Thus $R_k(\bar{\hat{f}}_1, \hat{f}_2, .., \hat{f}_n) = 0$. Hence any $(\xi) \in \ddot{V}$ annihilates $R_k(\bar{f}_1, f_2, .., f_n)$; whence $R_k(\bar{f}_1, f_2, .., f_n) \in \left\{R_k(g_1, f_2, .., f_n)\right\}$, so $R_k(g_1, f_2, .., f_n) \mid R_k(\bar{f}_1, f_2, .., f_n)$. In the same manner, we get that $R_k(h_1, f_2, .., f_n) \mid R_k(\bar{f}_1, f_2, .., f_n)$. But $R_k(g_1, f_2, .., f_n)$ and $R_k(h_1, f_2, .., f_n)$ are irreducible, and they are distinct since the first depends on the coefficients of g_1, while the second depends on the coefficients of h_1, and these coefficients are distinct. Since we are in a unique factorization domain we have

$$R_k(g_1, f_2, .., f_n) R_k(h_1, f_2, .., f_n) \mid R(g_1 h_1, f_2, .., f_n).$$

Now specialize f_1 into a product of linear forms. Then, applying the preceding result, we get that $R_k(f_1, f_2, .., f_n)$ is divisible by d_1 resultants. Specializing f_2 into a product of linear forms, we get that $R_k(f_1, f_2, .., f_n)$ is divisible by $d_1 d_2$ resultants. Continuing in this manner to f_{n-1}, we get that $R_k(f_1, f_2, .., f_n)$ is divisible by $d_1 d_2 ... d_{n-1}$ resultants, each of which depends on the coefficients of f_n.

Therefore, the degree of $R_k(f_1, f_2, \ldots, f_n)$ in (e')

is at least $d_1 d_2 \ldots d_{n-1}$. Thus we have obtained a lower

estimate.

To show that this is the precise degree in (e'), it

suffices to give one element of the prime ideal of this degree.

That is, we must obtain an element $F(a, a_n, b, b_n, \ldots, e, e_n)$

which is zero whenever the related forms have a common non-

trivial solution, and which is of degree $d_1 d_2 \ldots d_{n-1}$ in (e'),

for we then know that F is in the prime ideal, and, hence,

divisible by the resultant, so the resultant must have degree

less than or equal $d_1 d_2 \ldots d_{n-1}$ in (e').

We now proceed to construct such an F. We set

$d = \sum_{i=1}^{n} (d_i - 1) + 1$. Let μ_1 range over all monomials such

that $\mu_1 x_1^{d_1}$ has degree d. Let μ_2 range over all monomials

such that $\mu_2 x_2^{d_2}$ has degree d and such that $\mu_2 x_2^{d_2}$ does

not equal any of the preceding monomials; similarly for

$\mu_3, \ldots, \mu_n$. We claim that in this way we have exhausted

all monomials of degree d. For otherwise, a monomial would

have to be of the form $x_1^{\nu_1} x_2^{\nu_2} \ldots x_n^{\nu_n}$ where all $\nu_i \leq d_i - 1$,

so $\sum_{i=1}^{n} \nu_i < d$, and our contention is established.

Now, let us calculate the number of μ_n, which we will

denote by $\#(\mu_n)$.

$$\mu_n x_n^{d_n} = x_1^{\nu_1} x_2^{\nu_2} \ldots x_{n-1}^{\nu_{n-1}} x_n^{\nu_n}$$

where $\nu_1 + \nu_2 + \ldots + \nu_n = d$, and where $\nu_1 \leq d_1-1$, $\nu_2 \leq d_2-1$, $\ldots$, $\nu_{n-1} \leq d_{n-1}-1$ (so that the monomial did not appear earlier). Thus we see that

$$\#(\mu_n) = d_1 d_2 \ldots d_{n-1} ,$$

and, clearly,

$$\#(\mu_1, \mu_2, \ldots, \mu_n) = \text{the number of coefficients in}$$

a general form of degree d.

We now express all $f_1\mu_1$ (where f_1 is a form of degree d_1) as a sum of monomials of degree d, where we write 0 as a coefficient for a monomial which doesn't occur. We do the same thing for all $f_2\mu_2$, etc. Thus we have

$$f_1\mu_1 = \text{sum of monomials of degree d}$$

$$\cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots$$

$$f_2\mu_2 = \quad " \quad " \quad " \quad " \quad " \quad "$$

$$\cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots$$

$$\cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots$$

$$f_n\mu_n = \quad " \quad " \quad " \quad " \quad " \quad "$$

$$\cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots$$

The totality of terms occurring on the left hand side is $\#(\mu_1, \mu_2, \ldots, \mu_n)$ in number. Hence, we can view the co-efficients of the right hand side as a square matrix $(\#(\mu_1, \ldots, \mu_n) \times \#(\mu_1, \ldots, \mu_n))$. We claim that the desired polynomial, F, is the determinant of this matrix. Assume, for the moment, that we have shown that this polynomial is not identically zero. Then let us show that this

polynomial has the desired properties. Since the (e')
occur only in the $f_n \mu_n$, and since $\#(\mu_n) = d_1 d_2 \ldots d_{n-1}$, we
know that the (e') appear only in the last $d_1 d_2 \ldots d_{n-1}$
rows, so that the degree of the polynomial is $d_1 d_2 \ldots d_{n-1}$
in (e"). Now, let us show that this polynomial is divisible
by the resultant. Suppose $\hat{f}_1$, $\hat{f}_2 \ldots$, $\hat{f}_n$ (specialized forms
of degree d_1, .., d_n) have a common non-trivial solution.
Substitute, on the left side of (2.1), in the f_i these
coefficients and the solution. Then on the left hand side
of (2.1) we get all zeros. On the right hand side, we get
sums of specialized coefficients times monomials. Viewing
this as a system of linear equations (not identically zero),
we see that we have a system of linear equations with a non-
trivial solution. Hence, the determinant vanishes, but this
determinant is just the original determinant with specialized
values substituted. Thus we get the desired result.

Consequently, it only remains for us to show that the
determinant is not identically zero. If it were identically
zero, then it would be zero for every specialized choice of
the forms. Choose $f_1 = x_1^{d_1}$, $f_2 = x_2^{d_2}$, ..., $f_n = x_n^{d_n}$. Then
the totality of terms on the left hand side of (2.1) is just
the set of all monomials of degree d. Thus the determinant,
in this case, is just

$$
\begin{vmatrix}
1 & 0 & . & . & . & . & . & 0 \\
0 & 1 & 0 & . & . & . & .. & 0 \\
. & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . \\
0 & 0 & . & . & . & . & . & 1
\end{vmatrix} ,
$$

so for this particular choice, the determinant equals
$1 \neq 0$, which is a contradiction and completes the proof.

We now have a computational method of obtaining the
resultant; namely, calling the determinant that we obtained
$D_{e'}$, we may form $D_{a'}$, $D_{b'}$, ... by rearranging the forms in
(2.1) so that first f_1 then f_2 etc. occupy the last place.
We then would get that $D_{a'}$ has degree $d_2d_3...d_n$ in (a'), $D_{b'}$
has degree $d_1d_3...d_n$ in (b'), etc. Also, we get that
$D_{a'}$, $D_{b'}$, ..., $D_{e'}$ are each divisible by the resultant, and
finally that the resultant has degree $d_2d_3...d_n$ in (a'),
degree $d_1d_3...d_n$ in (b'), etc. Finally, since the resultant has
the highest degree which any common divisor of $D_{a'}$, $D_{b'}$, ..., $D_{e'}$
can have, we get that the resultant is the greatest common
divisor of the polynomials $D_{a'}$, $D_{b'}$, ..., $D_{e'}$. We can also see
now that the resultant is independent of the field k since it
is the greatest common divisor of the polynomials $D_{a'}$, $D_{b'}$, ...,
$D_{e'}$ in the ring $Z[a, a_n, b, b_n, ..., e, e_n]$ where Z designates the
ring of integers.

This concludes our introduction to the elements of
algebraic geometry, but the interested reader is strongly
urged to read A. Weil's <u>Foundations of Algebraic Geometry</u>
(A.M.S. Colloquium Publications) for further considerations.